モバイルデバイスの Cisco Secure Client

モバイルデバイスの Cisco Secure Client は、Windows、macOS、および Linux プラットフォームの Cisco Secure Client に似ています。この章では、モバイルデバイスでの Cisco Secure Client に固有のデバイス情報、設定情報、サポート情報、およびその他の管理タスクについて説明します。

モバイルデバイスでの Cisco Secure Client の動作およびオプション

Cisco Secure Client Mobile VPN 接続について

このリリースの Cisco Secure Client は、次のモバイルプラットフォームに対応しています。

- Android
- Apple iOS
- Chromebook
- Windows Phone

Cisco Secure Client は、サポートされている各プラットフォームのアプリストアに用意されています。www.cisco.com では入手できません。また、セキュリティで保護されたゲートウェイから配布されていません。

Cisco Secure Client モバイルアプリには、コア VPN クライアントのみが含まれています。Network Access Manager、ポスチャ（Secure Firewall ポスチャ または ISE ポスチャ）などの他の Cisco Secure Client モジュールは含まれていません。VPN が接続中の場合は、モバイルポスチャと呼ばれるポスチャ情報が、AnyConnect Identifier Extensions（ACIDex）を使用してヘッドエンドに提供されます。

Cisco Secure Client VPN 接続は、次のいずれかの方法で確立できます。

- ユーザが手動で確立する。
- ユーザが管理者により提供された自動接続アクションをクリックする際に手動で確立する（Android および Apple iOS のみ）。
- 自動：Connect on-Demand 機能により確立される（Apple iOS のみ）。

モバイルデバイスでの Cisco Secure Client VPN 接続エントリ

接続エントリは、セキュア ゲートウェイのアドレスを完全修飾ドメイン名または IP アドレス（必要に応じてトンネル グループ URL を含む）で識別します。また、他の接続属性を含めることもできます。

Cisco Secure Client では、1 台のモバイルデバイス上の複数の接続エントリをサポートすることで、異なるセキュア ゲートウェイや VPN トンネルグループに対応します。複数の接続エントリが設定されている場合は、VPN 接続を開始するためにユーザがどれを使用するかを理解することが重要です。接続エントリは次の方法のいずれかで設定されます。

- ユーザが手動で設定します。モバイル デバイスの接続エントリを設定する手順については、該当するプラットフォームのユーザ ガイドを参照してください。
- ユーザが管理者により提供されたリンクをクリックした後で追加し、接続エントリを設定します。

  ユーザにこの種の接続エントリ設定を提供するには、「VPN 接続エントリの生成 （40 ページ）」を参照してください。
- Cisco Secure Client VPN クライアントプロファイルで定義されます。

  Cisco Secure Client VPN クライアントプロファイルでは、クライアント動作を指定し、VPN 接続エントリを定義します。詳細については、「Cisco Secure Client VPN プロファイルでのモバイルデバイス接続の設定 （38 ページ）」を参照してください。

トンネリング モード

Cisco Secure Client は、マネージド BYOD またはアンマネージド BYOD 環境で動作可能です。これらの環境での VPN トンネリングは、次のいずれかのモードでのみ動作します。

- システム トンネリング モード：VPN 接続が、すべてのデータをトンネリングするために（完全トンネリング）、または特定のドメインまたはアドレスとの間で送受信されるデータのみをトンネリングするために（スプリット トンネリング）使用されます。このモードは、すべてのモバイル プラットフォームで使用できます。
- アプリケーションごとの VPN モード：VPN 接続は、モバイルデバイス（Android と Apple iOS のみ）上の特定のアプリケーションセットで使用されます。

  Cisco Secure Client では、管理者によってヘッドエンドで定義されているアプリケーションのセットを使用できます。このリストを定義するには、Cisco Secure Firewall ASA のカスタム属性のメカニズムを使用します。このリストは Cisco Secure Client に送信され、デバイスで適用されます。他のすべてのアプリケーションに対しては、データはトンネルを介さずに、または暗号化されずに送信されます。

  Apple iOS でこのモードで実行するには、マネージド環境が必要です。Android では、マネージドとアンマネージドの両方の環境がサポートされます。いずれのプラットフォームでも、マネージド環境では、Cisco Secure Client でトンネリングするように設定されている一連のアプリケーションと同じアプリケーションをトンネリングするように Mobile Device Manager でデバイスを設定する必要があります。
- マルチトンネル：iOS 上の Cisco Secure Client は、次のパターンを使用して複数のトンネルをサポートします。
  - 1 つの通常の（アプリケーションごとではない）VPN トンネルと、一度に接続された 1 つ以上のアプリケーションごとのトンネル
  - 一度に接続されたアプリケーションごとの VPN トンネルの数

  追加情報については、「iOS 向けの複数のトンネル （3 ページ）」を参照してください。

Cisco Secure Client Cisco Secure Firewall ASA ヘッドエンドから受信した設定情報によって決定されるモードで動作します。具体的には、接続に関連付けられたグループポリシーまたはダイナミック アクセス ポリシー（DAP）内のアプリごとの VPN リストの有無です。アプリケーション単位 VPN のリストが存在する場合、Cisco Secure Client はアプリケーション単位 VPN モードで動作し、存在しない場合は Cisco Secure Client はシステム トンネリング モードで動作します。

iOS 向けの複数のトンネル

ユーザーは、1 つのトンネルに対して 1 つの VPN 接続しか手動で開始できません（アプリケーションごとの VPN を使用する、または使用しない、いずれの場合も）。アプリケーションごとの VPN は関連付けられたアプリケーションで自動的に開始されるため、マルチトンネルを使用するには、MDM VPN プロファイルの VendorConfig に **MultiTunnel** キーを追加し、それを **true** に設定する必要があります。

iOS Cisco Secure Client のホーム画面には、接続されているかどうかに関係なく、選択したトンネルを示す表が表示されます。2 番目の表はダイナミックで、アプリケーションごとの VPN が接続されている場合にのみ表示されます。この 2 番目の表には、ユーザが [ステータス（Status）]

をクリックして、送受信されたバイト数とともに接続の [詳細な統計情報（Detailed Statistics）] を表示するまで、アプリケーションごとのトンネルの接続ステータスのみが表示されます。

現在選択されている通常の VPN のログの [診断（Diagnostics）] を参照できます。ユーザがログを共有することを決定した場合、ログパッケージには、接続されている VPN 設定のすべての VPN デバッグログファイルが含まれます。

モバイル デバイスでのセキュア ゲートウェイ認証

信頼されていないサーバのブロック

VPN 接続を確立するときに、Cisco Secure Client はセキュアゲートウェイから受信したデジタル証明書を使用してサーバーの身元を確認します。サーバ証明書が無効な場合（期限切れか無効な日付、キーの誤用、名前の不一致により証明書エラーがある）、または信頼できない場合（認証局が確認できない）場合、接続はブロックされます。ブロッキング メッセージが表示されるため、ユーザーは処理を選択する必要があります。

[信頼されていないサーバーをブロック（Block Untrusted Servers）] アプリケーション設定は、セキュア ゲートウェイを識別できない場合、Cisco Secure Client がどのように反応するかを決定します。この保護はデフォルトではオンです。ユーザーはオフにできますが、これは推奨されません。

[信頼されていないサーバをブロック（Block Untrusted Servers）] がオンの場合、信頼できない VPN サーバをブロックするという通知によって、ユーザーにセキュリティ上の脅威が警告されます。ユーザーは以下を選択できます。

- [安全を確保（Keep Me Safe）] を選択して、この接続を終わらせ、安全にしておきます。
- [設定の変更（Change Settings）] を選択して、[信頼されていないサーバをブロック（Block Untrusted Servers）] アプリケーション プリファレンスをオフにします。ただし、これは推奨されません。ユーザーがこのセキュリティ保護を無効にすると、VPN 接続を再起動しなくてはなりません。

[信頼されていないサーバをブロック（Block Untrusted Servers）] がオフの場合、信頼できない VPN サーバをブロックしないという通知によって、ユーザーにセキュリティ上の脅威が警告されます。ユーザーは以下を選択できます。

- [キャンセル（Cancel）] を選択して、接続をキャンセルし、安全にしておきます。
- [続行（Continue）] を選択して、接続を続行します。ただし、これは推奨されません。
- [詳細の表示（View Details）] を選択して、証明書の詳細を表示して受け入れるかどうかを判断します。

  ユーザーが確認している証明書が有効であるが信頼できない場合、ユーザーは次のことを実行できます。

  - 再使用できるようにサーバー証明書を Cisco Secure Client 証明書ストアにインポートし、[インポートおよび継続（Import and Continue）] を選択して接続を継続します。

Cisco Secure Client ストアにこの証明書がインポートされると、このデジタル証明書を使用しているそのサーバーに対する後続の接続は自動的に受け入れられます。

- 前の画面に戻り、[キャンセル（Cancel）] または [続行（Continue）] を選択します。

証明書が無効な場合、または何らかの理由で、ユーザーが前の画面にだけ戻ることができる場合、[キャンセル（Cancel）] または [続行（Continue）] を選択します。

VPN 接続の最も安全な設定では、[信頼されていないサーバーをブロック（Block Untrusted Servers）] の設定をオン（デフォルト設定）のままにし、自身のセキュアゲートウェイで設定された（有効で信頼できる）サーバー証明書を所有し、モバイルユーザーには常に [安全を確保（Keep Me Safe）] を選択させる必要があります。

（注） [厳格な証明書トラスト（Strict Certificate Trust）] はこの設定を上書きします（以下の説明を参照）。

OCSP 失効

Cisco Secure Client は OCSP（オンライン証明書状態プロトコル）をサポートします。これにより、OCSP レスポンダに要求を行い OCSP 応答を解析して証明書のステータスを取得することで、クライアントはリアルタイムで個々の証明書のステータスを照会できます。OCSP は、証明書チェーン全体を確認するために使用されます。OCSP レスポンダにアクセスする際、証明書ごとに 5 秒のタイムアウト間隔があります。

ユーザーは Cisco Secure Client 設定アクティビティで OCSP 検証を有効または無効にすることができます。MDM 管理者がリモートでこの機能を制御するために使用できる新しい API がフレームワークに追加されました。現在、Samsung と Google MDM がサポートされています。

厳格な証明書トラスト

ユーザーによって有効にされた場合、リモート セキュリティ ゲートウェイの認証時に Cisco Secure Client は確認できない証明書を許可しません。これらの証明書を受け入れるようユーザーにプロンプトを表示するのではなく、クライアントはセキュリティ ゲートウェイへの接続に失敗します。

（注） この設定は、[信頼されていないサーバをブロック（Block Untrusted Servers）] よりも優先されます。

オフにすると、クライアントはユーザーに証明書を受け入れるように求めます。これはデフォルトの動作です。

以下の理由があるため、Cisco Secure Client の厳格な証明書トラストを有効にすることを、強くお勧めします。

- 明確な悪意を持った攻撃が増えているため、ローカルポリシーで厳格な証明書トラストを有効にすると、パブリックアクセスネットワークなどの非信頼ネットワークからユーザーが接続している場合に「中間者」攻撃を防ぐために役立ちます。
- 完全に検証可能で信頼できる証明書を使用する場合でも、Cisco Secure Client は、デフォルトでは、未検証の証明書の受け入れをエンドユーザーに許可します。エンドユーザーが中間者攻撃の対象になった場合は、悪意のある証明書を受け入れるようエンドユーザーに求めます。エンドユーザーによるこの判断を回避するには、厳格な証明書トラストを有効にします。

モバイル デバイスでのクライアント認証

VPN 接続を完了するには、ユーザはユーザ名とパスワード、もしくはデジタル証明書、またはその両方の形式でクレデンシャルを提供して認証する必要があります。管理者は、トンネル グループの認証方式を定義します。モバイルデバイスでの最適なユーザーエクスペリエンスを達成するために、認証設定に応じて複数の Cisco Secure Client 接続プロファイルを使用することをお勧めします。ユーザエクスペリエンスとセキュリティのバランスを最適に保つ方法を決める必要があります。推奨事項は次のとおりです。

- モバイルデバイスの AAA 対応認証トンネル グループについては、クライアントを再接続状態にし、ユーザが再認証しなくても済むよう、グループ ポリシーは 24 時間など非常に長時間のアイドル タイムアウトが必要になります。
- 最もトランスペアレントなユーザエクスペリエンスを達成するには、証明書のみの認証を使用します。デジタル証明書を使用すると、VPN 接続は、ユーザとの対話なしで確立されます。

証明書を使用してセキュア ゲートウェイにモバイル デバイスを認証するため、エンド ユーザは、デバイスに証明書をインポートする必要があります。インポートすると、この証明書が自動証明書選択の対象として有効になり、特定の接続エントリに手動で関連付けることもできるようになります。証明書は、次の方法を使用してインポートされます。

- ユーザが手動でインポートします。モバイルデバイスに証明書をインポートする手順については、適切なユーザ ガイドを参照してください。
- SCEP を使用します。詳細については、「証明書登録の設定」を参照してください。
- 証明書をインポートするために管理者により提供されたリンクをユーザがクリックした後に追加されます。

  ユーザにこの種の証明書展開を提供するための詳細については、「証明書のインポート（47 ページ）」を参照してください。

モバイル デバイスでのローカリゼーション

Android および Apple iOS 用 Cisco Secure Client は、ローカリゼーションをサポートし、Cisco Secure Client ユーザーインターフェイスやメッセージをユーザーのロケールに適用しています。

パッケージ済みのローカリゼーション

Cisco Secure Client Android および Apple iOS アプリには、次の言語訳が含まれます。

- カナダ フランス語（fr-ca）
- 中国語（台湾）（zh-tw）
- チェコ語（cs-cz）
- オランダ語（nl-nl）
- フランス語（fr-fr）
- ドイツ語（de-de）
- ハンガリー語（hu-hu）
- イタリア語（it-it）
- 日本語（ja-jp）
- 韓国語（ko-kr）
- 中南米スペイン語（es-co）
- ポーランド語（pl-pl）
- ポルトガル語（ブラジル）（pt-br）
- ロシア語（ru-ru）
- 簡体字中国語（zh-cn）
- スペイン語（es-es）

Cisco Secure Client のインストール時には、これらの言語のローカリゼーションデータがモバイルデバイスにインストールされます。モバイルデバイスで指定されたロケールによって、表示される言語が決まります。Cisco Secure Client は、言語仕様、次に地域仕様を使用して、最適な一致を決定します。たとえば、インストール後にロケール設定をスイスフランス語（fr-ch）にすると、カナダ フランス語（fr-ca）表示になります。Cisco Secure Client の UI とメッセージは、Cisco Secure Client の起動時に変換されます。

ダウンロードされたローカリゼーション

Cisco Secure Client パッケージにはない言語に関して、管理者は、AnyConnect VPN 接続のデバイスにダウンロードされるローカライズデータを Cisco Secure Firewall ASA に追加します。

シスコは、Cisco.com の製品ダウンロードセンターで、ローカライズ可能なすべての Cisco Secure Client の文字列を含む anyconnect.po ファイルを提供しています。 Cisco Secure Client の管理者は anyconnect.po ファイルをダウンロードし、利用可能な文字列の翻訳を提供してから、ファイルを Secure Firewall ASA にアップロードします。Cisco Secure Firewall ASA に anyconnect.po ファイルがすでにインストールされている場合、Cisco Secure Client の管理者は更新バージョンをダウンロードします。

初期状態では、Cisco Secure Client ユーザーインターフェイスおよびメッセージがインストールした言語でユーザーに表示されます。デバイスユーザーが Cisco Secure Firewall ASA への初めての接続を確立すると、Cisco Secure Client では、デバイスの優先言語と Cisco Secure Firewall ASA 上で使用可能なローカリゼーション言語が比較されます。Cisco Secure Client で一致するローカリゼーションファイルが検索されると、ローカライズされたファイルがダウンロードされます。ダウンロードが完了すると、Cisco Secure Client は anyconnect.po ファイルに追加された変換文字列を使用してユーザーインターフェイスおよびユーザーメッセージを表示します。文字列が翻訳されていない場合、Cisco Secure Client ではデフォルトの英語文字列が表示されます。

Cisco Secure Firewall ASA でのローカリゼーションの設定手順については、「Cisco Secure Firewall ASA への変換テーブルのインポート」を参照してください。Cisco Secure Firewall ASA にデバイスのロケールのローカリゼーションデータが含まれていない場合、Cisco Secure Client アプリケーションパッケージにプリインストールされたローカリゼーションデータを引き続き使用します。

モバイル デバイスにローカリゼーションを提供するその他の方法

ユーザに URI リンクを提供することにより、Cisco Secure Client UI とメッセージのローカライズ （48 ページ）を実行します。

モバイル デバイスのユーザに、所有するデバイスでのローカリゼーション データの管理を依頼します。次のローカリゼーション アクティビティを実行する手順については、該当するユーザ ガイドを参照してください。

- 指定したサーバからのローカリゼーション データのインポート。ユーザは、ローカリゼーション データのインポートを選択し、セキュア ゲートウェイのアドレスとロケールを指定します。ロケールは ISO 639-1 で指定されており、適用可能な場合には国コードが追加されます（たとえば、en-US、fr-CA、ar-IQ など）。このローカリゼーション データは、インストールされたローカリゼーション データの代わりに使用されます。
- デフォルトのローカリゼーション データのリストア。Cisco Secure Client パッケージから事前ロードされたローカリゼーションデータの使用を復元し、インポートされたローカリゼーションデータをすべて削除します。

SAML を使用した VPN 認証

以下のリリースで、SAML 2.0 のサポートがモバイルデバイスに追加されました。SAML 認証を使用した場合、Cisco Secure Client セッションのみに適用されます。Web サイト、ブラウザが開始した SAML ログイン、またはインストールされているアプリケーションには適用されません。中断のないシームレスな再接続を提供するために、Cisco Secure Client は意図的に SAML 認証プロセスの繰り返しをスキップします。さらに、ユーザーがブラウザを使用して IdP からログアウトしても、Cisco Secure Client セッションは維持されます。

- iOS：バージョン 4.6。バージョン 4.8 では SAML とクライアント証明書
- Android：バージョン 4.6。バージョン 4.8 では SAML とクライアント証明書
- Chrome：バージョン 4.0

SAML を使用する場合は、次の注意事項に従ってください。

- フェールオーバーモードで常時接続の VPN を使用している場合、外部 SAML IdP はサポートされていません（ただし、内部 SAML IdP を使用すると、Cisco Secure Firewall ASA はすべてのトラフィックを IdP にプロキシします。また、ASA はサポートされています）。
- 信頼できないサーバー証明書は、組み込みブラウザでは許可されません。
- 組み込みブラウザ SAML 統合は、CLI モードまたは SBL モードではサポートされません。
- （モバイルのみ）単一ログアウトはサポートされていません。
- Web ブラウザに確立された SAML 認証は Cisco Secure Client と共有されず、その逆も同じです。
- 設定に応じて、組み込みブラウザ搭載のヘッドエンドに接続するときに、さまざまな方法が使用されます。たとえば、Cisco Secure Client では IPv6 接続よりも IPv4 接続の方が好ましく、組み込みブラウザでは IPv6 の方が好ましい場合もあります。あるいは、その逆もあります。同じく、プロキシを試して障害が発生したのに Cisco Secure Client がどのプロキシにもフォールバックしない場合もあれば、プロキシを試して障害が発生した後で組み込みブラウザがナビゲーションを停止する場合もあります。
- SAML 機能を使用するためには、Secure Firewall ASA の Network Time Protocol（NTP）サーバーを IdP NTP サーバーと同期する必要があります。
- ASDM の VPN ウィザードは現在、SAML 設定をサポートしていません。
- SAML IdP *NameID* 属性は、ユーザのユーザ名を特定し、認証、アカウンティング、および VPN セッション データベースに使用されます。
- ユーザが SAML 経由で VPN セッションを確立するたびにアイデンティティ プロバイダー（IdP）による再認証を行う場合は、Cisco Secure Client プロファイルエディタ、プリファレンス（Part 1）で [自動再接続（Auto Reconnect）] を *ReconnectAfterResume* に設定する必要があります。
- 組み込みブラウザ搭載の Cisco Secure Client は VPN 試行のたびに新しいブラウザ セッションを使用するため、IDP が HTTP セッションクッキーを使用してログオン状態を追跡している場合には、毎回ユーザーの再認証が必要になります。この場合、**[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [クライアントレスSSL VPNアクセス（Clientless SSL VPN Access）] > [詳細（Advanced）] [シングルサインオンサーバー（Single Sign On Servers）] >** の [強制再認証（Force Re-Authentication）] は、Cisco Secure Client が開始した SAML 認証には影響しません。

設定の詳細については、適切なリリース（9.7 以降）の『Cisco ASA Series VPN CLI or ASDM Configuration Guide』[英語] の「*SAML 2.0*」の項を参照してください。

Cisco Secure Firewall ASA への変換テーブルのインポート

ステップ 1 www.cisco.com から目的の変換テーブルをダウンロードします。

ステップ 2 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect カスタマイゼーション/ローカリゼーション（AnyConnect Customization/Localization）] > [GUI テキストおよびメッセージ（GUI Text and Messages）]** に移動します。

ステップ 3 [インポート（Import）] をクリックします。[言語ローカリゼーションエントリのインポート（Import Language Localization Entry）] ウィンドウが表示されます。

ステップ 4 ドロップダウン リストから適切な言語を選択します。

ステップ 5 変換テーブルのインポート元を指定します。

ステップ 6 [今すぐインポート（Import Now）] をクリックします。この変換テーブルが、この優先言語で Cisco Secure Client クライアントに展開されます。ローカリゼーションは、Cisco Secure Client がリスタートし、再接続した後に適用されます。

モバイル デバイスでの FIPS および Suite B 暗号化

モバイルデバイス向け Cisco Secure Client には、Cisco Common Cryptographic Module（C3M）が組み込まれています。これは、新世代の暗号化（NGE）アルゴリズムの一部として FIPS 140-2 に準拠した暗号化モジュールや NSA Suite B 暗号化が含まれる Cisco SSL の実装です。Suite-B 暗号化は、IPSec VPN でのみ使用可能です。FIPS 準拠の暗号化は、IPSec VPN および SSL VPN の両方で使用可能です。

暗号化アルゴリズムを使用すると、接続の間、ヘッドエンドルータとネゴシエートされます。ネゴシエーションは、VPN 接続の両端の機能によって異なります。したがって、セキュア ゲートウェイは、FIPS に準拠する暗号化および Suite B の暗号化をサポートする必要があります。

ユーザーは、Cisco Secure Client アプリケーション設定の **FIPS モード**を有効にすることで、ネゴシエーションにおいて NGE アルゴリズムだけを受け入れるように Cisco Secure Client を設定します。FIPS モードが無効の場合、Cisco Secure Client は VPN 接続の非 FIPS 暗号アルゴリズムも受け入れます。

モバイルのその他のガイドラインと制限事項

- Apple iOS 5.0 以降が Suite B の暗号化に必要です。これは Suite B で使用される ECDSA の証明書をサポートする Apple iOS の最も低いバージョンです。
- Android 4.0（Ice Cream Sandwich）以降が Suite B の暗号化に必要です。これは、SuiteB で使用される ECDSA の証明書をサポートする Android の最も低いバージョンです。
- FIPS モードで動作しているデバイスには、プロキシ方式または従来の方法でデジタル証明書をモバイル ユーザに提供するための SCEP の使用との互換性がありません。状況に応じた展開計画を立ててください。

Android デバイスでの Cisco Secure Client

リリースごとの機能および更新については、『Release Notes for Cisco Secure Client, for Android』[英語] を参照してください。

このリリースでサポートされている機能およびデバイスについては、『Cisco Secure Client Mobile Platforms and Feature Guide』[英語] を参照してください。

Android での Cisco Secure Client の注意事項と制約事項

- Cisco Secure Firewall ASA は、Android 向け Cisco Secure Client のディストリビューションと更新プログラムを提供しません。Google Play から入手できます。最新バージョンの APK（パッケージ）ファイルも Cisco.com に掲載されています。
- Android 向け Cisco Secure Client は Network Visibility Module と Umbrella のみサポートし、他の Secure Client モジュールはサポートしていません。
- Android デバイスでは 1 つの Cisco Secure Client プロファイル（ヘッドエンドから受信した最後のプロファイル）だけがサポートされます。ただし、プロファイルは複数の接続エントリで構成できます。
- ユーザーが、サポートされていないデバイスに Cisco Secure Client をインストールしようとすると、「インストールエラー：原因不明 -8（Installation Error: Unknown reason -8）」というポップアップメッセージが表示されます。これは Android OS により生成されるメッセージです。
- ユーザーがホームスクリーンに Cisco Secure Client ウィジェットを表示している場合、[起動時に開く（Launch at startup）] 設定に関わらず Cisco Secure Client サービスが自動的に開始されます（ただし接続は確立されません）。
- Android 向け Cisco Secure Client では、クライアント証明書からの事前入力を使用する場合に、拡張 ASCII 文字のために UTF-8 文字エンコードが必要です。事前入力機能を使用する場合は、クライアント証明書が UTF-8 でなければなりません（KB-890772 および KB-888180 の説明を参照）。
- Cisco Secure Client は、EDGE の固有の性質およびその他の早期無線テクノロジーによって EDGE 接続上の VPN トラフィックを送受信する場合、ボイスコールをブロックします。
- いくつかのよく知られているファイル圧縮ユーティリティでは、[Cisco Secure Client 送信ログ（AnyConnect Send Log）] ボタンを使用してパッケージされたログバンドルを圧縮解除できません。回避策として、Cisco Secure Client ログファイルの圧縮解除には Windows および macOS のネイティブユーティリティを使用してください。
- DHE の非互換性：Cisco Secure Client で導入された DHE 暗号サポートにより、ASA 9.2 より前の Cisco Secure Firewall ASA バージョンで非互換性の問題が発生します。9.2 より前の Cisco Secure Firewall ASA リリースで DHE 暗号を使用している場合、これらの Cisco Secure Firewall ASA バージョンで DHE 暗号を無効にする必要があります。

- Cisco Secure Client はネットワーク VPN アプリケーションであるため、機能するにはバックグラウンド操作が必要です。そのため、絶対に Cisco Secure Client をディープスリープリストに追加しないでください。

Android 固有の考慮事項

Android モバイル ポスチャ デバイスの ID 生成

新規インストール時、またはユーザーがアプリケーションデータを消去した後、Cisco Secure Client は Android ID に基づいて 256 バイトの一意のデバイス ID を生成します。この ID は、以前のリリースで生成された IMEI と MAC アドレスに基づく 40 バイトのレガシー デバイス ID を置き換えます。

Cisco Secure Client の以前のバージョンがインストールされている場合、レガシー ID はすでに生成されています。Cisco Secure Client のこのバージョンにアップグレードすると、ユーザーがアプリケーションデータを消去するか Cisco Secure Client をアンインストールするまで、このレガシー ID は引き続きデバイスの固有 ID として報告されます。

生成されたデバイス ID は、アプリケーションの初回起動時に、Cisco Secure Client の **[診断（Diagnostics）] > [ログインとシステム情報（Logging and System Information）] > [システム（System）] > [デバイス識別子（Device Identifiers）]** 画面、`device_identifiers.txt` ファイルの Cisco Secure Client ログ、または [バージョン情報（About）] 画面から参照できます。

（注） セキュア ゲートウェイ上の DAP ポリシーは、新しいデバイス ID を使用するように更新する必要があります。

`Device-ID` は、次のように決定されます。

```
Device-ID = bytesToHexString(SHA256(Android-ID))
```

ここで、`Android ID` と `bytesToHexString` は次のように定義されます。

```
Android-ID = Secure.getString(context.getContentResolver(), Secure.ANDROID_ID)
```

```
String bytesToHexString(byte[] sha256rawbytes){
String hashHex = null;
if (sha256rawbytes != null){
  StringBuffer sb = new StringBuffer(sha256rawbytes.length * 2);
    for (int i = 0; i < sha256rawbytes.length; i++){
    String s = Integer.toHexString(0xFF & sha256rawbytes[i]).toUpperCase();
    if (s.length() < 2) {sb.append("0");}
    sb.append(s);
    }
  hashHex = sb.toString();
  }
return hashHex; }
```

Android デバイスのアクセス許可

次のアクセス許可が AnyConnect の動作用に Android マニフェスト ファイルで宣言されます。

マニフェストのアクセス許可	説明
uses-permission: android.permission.ACCESS_NETWORK_STATE	アプリケーションがネットワークの情報にアクセスすることを許可します。
uses-permission: android.permission.ACCESS_WIFI_STATE	アプリケーションが Wi-Fi ネットワークの情報にアクセスすることを許可します。
uses-permission: android.permission.BROADCAST_STICKY	アプリケーションがスティッキ インテントをブロードキャストすることを許可します。これは、クライアントが次のブロードキャストを待たなくてもデータをすぐに取得できるよう、完了後もデータがシステムによって保持されるブロードキャストです。
uses-permission: android.permission.INTERNET	アプリケーションがネットワーク ソケットを開くことを許可します。
uses-permission: android.permission.READ_EXTERNAL_STORAGE	アプリケーションが外部ストレージから読み取ることを許可します。
uses-permission: android.permission.READ_LOGS	アプリケーションが低レベルのシステム ログ ファイルを読み取ることを許可します。
uses-permission: android.permission.READ_PHONE_STATE	デバイスの電話番号、現在の携帯電話ネットワーク情報、通話中のコールのステータス、デバイスに登録されているすべての PhoneAccounts のリストなどの電話状態への読み取り専用アクセスを許可します。
uses-permission: android.permission.RECEIVE_BOOT_COMPLETED	システムの起動完了後にアプリケーションがブロードキャストを受信することを許可します。

Chromebook での Android 向け Cisco Secure Client の設定

Google は最近、すべてのネイティブ Chromebook アプリケーションの廃止を発表しました。この手順は、ネイティブ Chromebook アプリケーションからの移行、および Chromebook での Android 向け Cisco Secure Client の設定に役立ちます。

詳細については、この Google のマニュアルを参照してください。

ステップ 1 管理者アカウントを使用して Google 管理コンソールにサインインします。

ステップ 2 Google 管理コンソールのホームページで、[Devices] > [Chrome] に移動します。

ステップ 3 [Apps & extensions] > [Users & browsers] をクリックします。

ステップ 4 設定を全員に適用する場合は、最上位の組織部門を選択したままにします。それ以外の場合は、子組織単位を適用します。

ステップ 5 [Add] > [Add from Google Play] をクリックします。

ステップ 6 管理するアプリケーションとして [Cisco Secure Client] を選択します。

ステップ 7 管理対象の設定はJSONファイルのみで、これを貼り付けるか、アップロードアイコンをクリックしてアップロードできます。

次のタスク

キーは、Android の .apk パッケージファイルで定義されます。唯一の必須フィールドは vpn_connection_host ですが、Cisco Secure Client XML プロファイルをプッシュする場合、JSON キーは vpn_connection_profile です。Cisco Secure Client は、次のセクションに示すすべての管理対象設定キーをサポートします。

Cisco Secure Client でサポートされる管理対象設定キー

管理対象制限事項（ルート）

vpn_connection_name

- タイトル：接続名
- 型：String
- 説明：ユーザにわかりやすい名前（表示専用）。設定されていない場合は、デフォルトでホストになります。

vpn_connection_host

- タイトル：ホスト
- 型：string
- 説明：ヘッドエンドへの URL。このフィールドは必須です。

vpn_connection_profile

- タイトル：プロトコル
- 型：choice
- 設定可能な値：SSL | IPsec
- 説明：VPN トンネルプロトコル（SSL または IPsec）。デフォルトは SSL

vpn_connection_ipsec_auth_mode

- タイトル：IPsec 認証モード
- 型：choice

- 説明：（任意）トンネルプロトコルが IPsec の場合に使用する認証モード。デフォルトは EAP-AnyConnect

vpn_connection_ipsec_ike_identity

- タイトル：IKE ID
- 型：string
- 説明：（任意）IPsec 認証モードが EAP_GTC、EAP-Md5、または EAP-MSCHAPv2 の場合にのみ適用されます

vpn_connection_ipsec_ike_identity

- タイトル：IKE ID
- 型：string
- 説明：（任意）IPsec 認証モードが EAP_GTC、EAP-MD5、または EAP-MSCHAPv2 の場合にのみ適用されます。

vpn_connection_keychain_cert_alias

- タイトル：キーチェーン証明書エイリアス
- 型：string
- 説明：（任意）この VPN 設定に使用するクライアント証明書のキーチェーンエイリアス。

vpn_connection_allowed_apps

- タイトル：アプリケーションごとの VPN 許可アプリケーション
- 型：string
- 説明：（任意）トンネリングするアプリ（Android アプリパッケージ名のカンマ区切りリスト）を指定します。これにより、アプリごとの VPN が有効になります。他のすべてのアプリケーションはトンネリングされません。この設定では、ヘッドエンドでアプリケーションごとの VPN を有効にする必要があります。

vpn_connection_disallowed_apps

- タイトル：アプリケーションごとの VPN で許可されないアプリケーション
- 型：string
- 説明：（任意）トンネリングしないアプリ（Android アプリパッケージ名のカンマ区切りリスト）を指定します。これにより、アプリごとに VPN が有効になります。他のすべてのアプリケーションはトンネリングされます。この設定では、ヘッドエンドでアプリケーションごとの VPN を有効にする必要があります。

vpn_connection_allow_bypass

- タイトル：VPN トンネルのバイパスをアプリケーションに許可する

- タイプ：boolean
- 説明：（任意）この VPN 接続をバイパスすることをアプリに許可します。デフォルトでは無効になっています。

vpn_setting_replace_existing_profile

- タイトル：既存のプロファイルの置き換え
- 型：bool
- 説明：（任意）vpn_connection_profile が設定されている場合にのみ適用されます。クライアントにインストール済みのプロファイルを管理対象設定プロファイルで置き換えるかどうかを指定します。これを無効にすると、Cisco Secure Firewall ASA プッシュプロファイルとの競合を避けることができます。デフォルトでは有効になっています。

vpn_setting_apply_perapp_to_profile

- タイトル：アプリケーションごとのルールをプロファイルをインポートした構成に適用する
- 型：bool
- 説明：（任意）管理対象設定のアプリケーションごとの VPN ルール（存在する場合）を Cisco Secure Client プロファイル XML からインポートした設定に適用するかどうかを指定します。デフォルトでは無効になっています。

vpn_connection_set_active

- タイトル：アクティブに設定
- 型：bool
- デフォルト値：True
- 説明：（任意）これが最後に選択された VPN 設定として設定されます。

vpn_setting_fips_mode

- タイトル：FIPS モード
- 型：bool
- 説明：（任意）Cisco Secure Client の FIPS モードを有効にするかどうか。

vpn_setting_uri_external_control

- タイトル：URI 外部制御
- 型：string
- 説明：（任意）URI 処理（外部制御）を設定します。有効なオプションは、プロンプト、有効、および無効です。

vpn_setting_strict_mode

- タイトル：ストリクトモード
- 型：bool
- 説明：（任意）Cisco Secure Client の厳格な証明書トラストモードを有効にするかどうか。

vpn_setting_certificate_revocation

- タイトル：証明書の失効
- 型：bool
- 説明：（任意）Cisco Secure Client をチェックする OCSP サーバー証明書を有効にするかどうか。

vpn_connection_profile

- タイトル：Cisco Secure Client プロファイル
- 型：string
- 説明：（任意）インポートのための Cisco Secure Client プロファイル（XML 形式または XML の Base64 エンコーディング）

vpn_connection_device_id

- タイトル：デバイス ID
- 型：string
- 説明 ：（任意）ヘッドエンドへのデバイスレポートの識別子。設定されていない場合、Cisco Secure Client はランダムな永続デバイス ID を生成します。

vpn_connection_report_hardware_id

- タイトル：VPN 認証のハードウェア ID（MAC アドレスと IMEI）の報告
- 型：bool
- 説明：（任意）Cisco Secure Client がハードウェア ID をヘッドエンドに報告しようとするかどうかを指定します。デフォルトでは、Cisco Secure Client はアクセス可能なハードウェア ID を報告しようとします。

vpn_setting_allowed_saved_credentials

- タイトル：ユーザによるクレデンシャルの保存を許可
- 型：bool
- デフォルト値：false
- 説明：（任意）ユーザがクレデンシャルを保存できるようにするかどうか（画面ロックが必要）。デフォルトでは、ユーザはクレデンシャルを保存できません。

vpn_configuration_list

- タイトル：VPN 接続リスト
- 型：bundle_array
- 説明：（任意）これを使用して複数の接続エントリを設定します。各エントリは vpn_configuration バンドルです。

umbrella_org_id

- タイトル：Umbrella 組織 ID
- 型：string
- 説明：顧客が属する組織 ID。Cisco Umbrella ダッシュボードからダウンロードされた設定ファイルに表示されます。

umbrella_reg_token

- タイトル：Umbrella 登録トークン
- 型：string
- 説明：組織に発行された一意の regToken。値は、Cisco Umbrella ダッシュボードからダウンロードされた設定ファイルに表示されます。

umbrella_va_fqdns

- タイトル：Umbrella VA FQDN リスト
- 型：string
- 説明：これは、接続されたネットワークに存在する VA の FQDN リストです。

admin_email

- タイトル：管理者の電子メールアドレス
- 型：string
- 説明：（任意）ログを送信するためのデフォルトの管理者電子メールアドレスを設定します。

vpn_always_on_umbrella_only

- タイトル：VPN モードを Umbrella 保護に対してのみ常にオンにする
- 型：bool
- デフォルト値：false
- 説明：（Umbrella を使用する場合にのみ適用）true に設定すると、常にオンの VPN は Umbrella 保護にのみ適用されます。false に設定すると、常にオンの VPN は Umbrella とリモートアクセスの両方に適用されます。

block_user_create_vpn_connection

- タイトル：ユーザーが新しい VPN 接続を作成できないようにする
- タイプ：boolean
- 可能な値：true または false
- 説明：Cisco Secure Client ユーザーが新しい VPN 接続を作成できないようにするには、**block_user_create_vpn_connection** キーを true に設定します。デフォルトは false で、VPN 接続の作成を許可します。

vpn_setting_block_untrusted_servers

- タイトル：信頼されていないサーバーをブロックする
- タイプ：boolean
- 可能な値：true または false
- 説明：管理対象デバイスの [信頼されていないサーバーをブロック（Block Untrusted Server）] オプションを設定するには、**vpn_setting_block_untrusted_servers** キーを *true* に設定します。この設定では、ユーザーは信頼されていないサーバー証明書を持つサーバーに接続できません。デフォルトは False です。

accept_seula_for_user

- タイトル：ユーザーの SEULA に同意する
- タイプ：boolean
- 可能な値：true または false
- 説明：管理対象デバイスでエンドユーザーライセンス契約（EULA）を非表示にして、新しいユーザーのオンボーディングを容易にするには、**accept_seula_for_user** キーを *true* に設定します。この設定により、ユーザーはアプリの初回起動時にデフォルトの Cisco EULA 要件を満たさなくてもアクセスすることができます。デフォルトは False です。

vpn_connection_yubikey_cert_slot

- タイトル：Yubikey 証明書スロット
- 型：string
- 可能な値：9a、9c、9d、または 9e
- 説明：（オプション) 証明書認証に使用する Yubikey スロット（9a、9c、9d、または 9e）を指定します。

vpn_configuration バンドルの管理対象制限事項

vpn_name

- タイトル：表示名
- 型：string

- 説明：ユーザにわかりやすい名前（表示専用）。設定されていない場合は、デフォルトでホストになります。

vpn_host

- タイトル：ホスト
- 型：string
- 説明：ヘッドエンドへの URL。このフィールドは必須です。

vpn_protocol

- タイトル：プロトコル
- 型：choice
- 設定可能な値：SSL | IPsec
- 説明：VPN トンネルプロトコル（SSL または IPsec）。デフォルトは SSL です。

vpn_ipsec_auth_mode

- タイトル：IPsec 認証モード
- 型：choice
- 設定可能な値：EAP-AnyConnect | EAP-GTC | EAP-MD5 | EAP-MSCHAPv2 | IKE RSA
- 説明：（任意）トンネルプロトコルが IPsec の場合に使用する認証モード。デフォルトは EAP-Connect です。

vpn_ipsec_ike_identity

- タイトル：IKE ID
- 型：string
- 説明：（任意）IPsec 認証モードが EAP_GTC、EAP-MD5、または EAP-MSCHAPv2 の場合にのみ適用されます。

vpn_keychain_cert_alias

- タイトル：キーチェーン証明書エイリアス
- 型：string
- 説明：（任意）この VPN 設定に使用するクライアント証明書のキーチェーンエイリアス。

vpn_allowed_apps

- キー：vpn_allowed_apps
- タイトル：アプリケーションごとの VPN 許可アプリケーション
- 型：string

- 説明：（任意）トンネリングするアプリ（Android アプリパッケージ名のカンマ区切りリスト）を指定します。これにより、アプリごとの VPN が有効になります。他のすべてのアプリケーションはトンネリングされません。この設定では、ヘッドエンドでアプリケーションごとの VPN を有効にする必要があります。

vpn_disallowed_apps

- タイトル：アプリケーションごとの VPN で許可されないアプリケーション
- 型：string
- 説明：（任意）トンネリングしないアプリ（Android アプリパッケージ名のカンマ区切りリスト）を指定します。これにより、アプリごとの VPN が有効になります。他のすべてのアプリケーションはトンネリングされます。この設定では、ヘッドエンドでアプリケーションごとの VPN を有効にする必要があります。

vpn_allow_bypass

- タイトル：VPN トンネルのバイパスをアプリケーションに許可する
- 型：bool
- 説明：（任意）この VPN 接続をバイパスすることをアプリに許可します。デフォルトでは無効になっています。

vpn_set_active

- タイトル：アクティブに設定：
- 型：bool
- デフォルト値：false
- 説明：（任意）これが最後に選択された VPN 設定として設定されます。

vpn_yubikey_cert_slot

- タイトル：Yubikey 証明書スロット
- 型：string
- 可能な値：9a、9c、9d、または 9e
- 説明：（オプション）証明書認証に使用する Yubikey スロット（9a、9c、9d、または 9e）を指定します。

Apple iOS デバイスでの Cisco Secure Client

このリリースでサポートされている機能およびデバイスについては、『Release Notes for Cisco Secure Client, for Apple iOS』[英語] を参照してください。

Apple iOS での Cisco Secure Client の注意事項と制約事項

Apple iOS 用 Cisco Secure Client では、リモート VPN アクセスに関連する機能では、次の機能のみがサポートされます。

- Cisco Secure Client の設定は、ユーザー（手動で）によって、または Apple Configurator Utility（http://www.apple.com/support/iphone/enterprise/）によって生成する Cisco Secure Client VPN クライアントプロファイルによって行うか、エンタープライズ モバイル デバイス マネージャを使用して行うことができます。
- Apple iOS デバイスは 1 つの Cisco Secure Client VPN クライアントプロファイルのみサポートします。生成された設定の内容は、必ず最新のプロファイルと一致します。たとえば、vpn.example1.com に接続してから vpn.example2.com に接続します。vpn.example2.com からインポートされた Cisco Secure Client VPN クライアントプロファイルは、vpn.example1.com からインポートされたものを置き換えます。
- このリリースは、トンネルキープアライブ機能をサポートしています。ただし、デバイスのバッテリ寿命は短くなります。アップデート間隔の値を増やすことでこの問題は軽減します。

Apple iOS Connect On-Demand の注意事項：

- iOS On-Demand ロジックの結果として自動的に接続され、Disconnect on Suspend（一時停止時に接続解除）が設定されている VPN セッションは、デバイスがスリープすると切断されます。デバイスがスリープ状態から起動すると、必要に応じて On-Demand ロジックが VPN セッションを再接続します。
- Cisco Secure Client は、UI が起動され、VPN 接続が開始されたときにデバイス情報を収集します。そのため、ユーザーが iOS の Connect on Demand 機能を使用して最初に接続を行う場合、または OS バージョンなどのデバイス情報が変更された後、Cisco Secure Client がモバイルポスチャ情報を誤ってレポートする状況が発生します。

Apple iOS 固有の注意事項

Apple iOS デバイスで Cisco Secure Client をサポートする場合は、次の点を考慮してください。

- このマニュアルの SCEP の参照は、Apple iOS SCEP ではなく、Cisco Secure Client SCEP にのみ適用されます。
- Apple iOS に制約があるため、プッシュ電子メール通知は VPN では動作しません。ただし、Cisco Secure Client は、トンネルポリシーがこれらをセッションから除外する際に、外部にアクセスできる ActiveSync 接続と平行して作動します。
- iOS の Cisco Secure Client は、Siri、ショートカット、キーボードショートカットなどの iOS ユーザー補助機能を介して制御できます。OS への「Intents」のドネートを接続および切断する操作は、ショートカットアプリを備え、Siri（および/または他の自動化メカニズム）が有効な Cisco Secure Client を使用して管理されます。たとえば、ショートカットアプリ内で、新しいショートカットを作成し、Cisco Secure Client を検索して、[VPN の開始（Start

VPN）] を選択できます。その後、[再生（Play）] を押すと、ショートカットが実行され、デフォルトのプロンプトが表示されます。[VPN の停止（Stop VPN）] の同様のショートカットを作成でき、編集して色、グリフ、または順序を変更できます。エントリを展開し、[実行時に表示（Show When Run）] をオフにすることで、プロンプトを無効化することもできます。

iOS の Cisco Secure Client はサンドボックス アプリケーションであり、アプリケーションの外部でのユーザのキーストロークに直接アクセスすることはできません。ただし、サーバーとの接続および切断後は、Siri、ショートカット、およびキーボードショートカットを介して Cisco Secure Client を制御できます。iOS ショートカットとキーボードショートカットの使用方法については、iOS ユーザー補助機能を参照してください。

Apple Configurator ユーティリティ

Windows または macOS 向けに Apple から入手可能な iPhone 構成ユーティリティ（IPCU）を使用して、 構成を作成して、Apple iOS デバイスに展開できます。これは、セキュアゲートウェイの Cisco Secure Client プロファイル設定の代用にできます。

Apple で制御される既存の IPCU GUI は、Cisco Secure Client IPsec 機能を認識しません。IPCU の既存の Cisco Secure Client GUI 内で IPsec VPN 接続を設定します。RFC 2996 で定義されているように、次の URI 構文を [サーバ（Server）] フィールドに使用します。このサーバ フィールドの構文は SSL VPN 接続設定のドキュメント化された使用方法と下位互換性があります。

[**ipsec**://][<**AUTHENTICATION**> [」:「<**IKE-IDENTITY**>「@」]] <**HOST**> [」:「<**PORT**>] ["/"<**GROUP-URL**>]

パラメータ	説明
ipsec	IPSec 接続であることを示します。省略すると、SSL が使用されます。
AUTHENTICATION	IPSec 接続の認証方式を指定します。省略すると、EAP-AnyConnect が使用されます。有効な値は次のとおりです。 • EAP-AnyConnect • EAP-GTC • EAP-MD5 • EAP-MSCHAPv2 • IKE-RSA
IKE-IDENTITY	AUTHENTICATION が EAP-GTC、EAP-MD5 または EAP-MSCHAPv2 に設定されているとき、IKE ID を指定します。このパラメータは、他の認証設定に使用されたときに無効になります。
HOST	サーバ アドレスを指定します。使用するホスト名または IP アドレス。

パラメータ	説明
PORT	現在は無視されています。HTTP URI スキームとの一貫性のために含まれています。
GROUP=URL	サーバ名に付加されるトンネル グループ名。

次に例を示します。

```
ipsec://EAP-AnyConnect@asa-gateway.example.com
ipsec://asa-gateway.example.com
```

規格に準拠した Cisco IOS ルータにのみ接続するには、次を使用します。

```
ipsec://eap-md5:<identity>@ios-gateway.example.com
```

Connect-on-Demand の使用上のガイドライン

Apple iOS Connect On Demand 機能を使用すると、Safari などの他のアプリケーションで VPN 接続を開始できます。Apple iOS は、デバイスのアクティブな接続エントリに設定されたルールに対して、アプリケーションから要求されたドメインを評価します。Apple iOS は、次のすべての条件が満たされた場合にのみ、アプリケーションに代わって VPN 接続を確立します。

- VPN 接続がまだ確立されていない。
- Apple iOS Connect on Demand フレームワークに対応するアプリケーションがドメインを要求している。
- 接続エントリが有効な証明書を使用するように設定されている。
- 接続エントリで Connect on Demand が有効化されている。
- Apple iOS が、[接続しない（Never Connect）] リスト内の文字列とドメイン要求の照合に失敗する。
- 次のいずれかが該当します。Apple iOS は、[常に接続する（Always Connect）] リスト内の文字列をドメイン要求に照合します（Apple iOS 6 でのみ）。または、DNS ルックアップが失敗し、Apple iOS が、[必要に応じて接続（Connect if Needed）] リスト内の文字列をドメイン要求に照合します。

Connect On Demand 機能を使用する場合は、次の点に注意してください。

- iOS の Connect on Demand を使用して VPN 接続が開始された後、iOS は、トンネルが一定の期間非アクティブである場合、そのトンネルの接続を解除します。詳細については、Apple の『VPN Connect-on-Demand』[英語] のマニュアルを参照してください。
- 規則を設定する場合は、[必要に応じて接続（Connect if Needed）] オプションを指定することをお勧めします。[必要に応じて接続（Connect if Needed）] ルールは、内部ホストへの DNS ルックアップに失敗した場合に VPN 接続を開始します。企業内のホスト名が内部 DNS サーバを使用してのみ解決されるよう、正しく DNS 設定を行う必要があります。
- 設定された Connect on Demand があるモバイル デバイス用に、証明書ベースの認証トンネル グループに短時間（60 秒）のアイドル タイムアウト（vpn-idle-timeout）が必要です。

VPNセッションがアプリケーションにとって重大な問題がなく、常時接続が必要ではない場合は、アイドル タイムアウトを短く設定します。デバイスがスリープ モードに移行するなど必要でなくなった場合、Apple デバイスは VPN 接続を閉じます。トンネル グループのデフォルト アイドル タイムアウトは 60 分です。

- 常時接続動作は、リリースに依存します。
  - Apple iOS 6 では、iOS はこのリスト ルールが一致したときに常に VPN 接続を開始します。
  - iOS 7.x では、[常に接続する（Always Connect）] はサポートされていません。このリストのルールが一致しても、[必要に応じて接続（Connect if Needed）] のルールとして動作します。
  - 以降のリリースでは、[常に接続する（Always Connect）] は使用されません。設定済みのルールは [必要に応じて接続（Connect if needed）] リストに移動され、それに応じて動作します。
- Apple は、Connect-on-Demand 機能に Trusted Network Detection（TND）の拡張機能を導入しました。この機能拡張は次のとおりです。
  - デバイス ユーザが信頼ネットワーク内にいるかどうかを判断して、Connect-on-Demand 機能を拡張します。
  - Wi-Fi 接続だけに適用されます。他のタイプのネットワーク接続を介して動作している場合、Connect on Demand は、VPN を接続するかどうかを判断するために TND を使用しません。
  - 個々の機能はなく、Connect-on-Demand 機能の外で設定または使用できません。

  iOS 6 の Connect-on-Demand 信頼ネットワーク検出に関する情報は、Apple にお問い合わせください。
- 統合された Apple iOS IPsec クライアントと Cisco Secure Client はどちらも、同じ Apple iOS VPN Connect-on-Demand フレームワークを使用します。

スプリット トンネルによるスプリット DNS 解決の動作

Cisco Secure Firewall ASA スプリットトンネリング機能では、VPN トンネルにアクセスするトラフィックや、クリアテキストで送信されるトラフィックを指定できます。スプリット DNS と呼ばれる関連機能は、VPN トンネル上の DNS 解決のために適切な DNS トラフィックや、エンドポイント DNS リゾルバが処理する DNS トラフィックを（クリアテキストで）指定できます。スプリットトンネリングも設定した場合、スプリット DNS は Apple iOS デバイスで他のデバイスとは異なる方法で機能します。Apple iOS 向け Cisco Secure Client は、このコマンドには次のように応答します。

- split-dns リストのドメインに対して、DNS クエリーだけを暗号化します。

  Cisco Secure Client は、コマンドで指定されたドメインの DNS クエリのみをトンネリングします。他のすべての DNS クエリはクリアテキストでローカル DNS リゾルバに送信し、

解決を行います。たとえば、Cisco Secure Client は次のコマンドに対して example1.com および example2.com の DNS クエリーのみトンネルします。

```
hostname(config-group-policy)# split-dns value example1.com example2.com
```

- default-domain コマンドのドメインに対して、DNS クエリーだけを暗号化します。

  split-dns none コマンドが存在し、**default-domain** コマンドがドメインを指定する場合、Cisco Secure Client はこのドメインに DNS クエリーだけをトンネルし、他の DNS クエリーすべてをローカル DNS リゾルバにクリアテキストで送信します。たとえば、Cisco Secure Client は次のコマンドに対して example1.com の DNS クエリーのみトンネルします。

```
hostname(config-group-policy)# split-dns none
hostname(config-group-policy)# default-domain value example1.com
```

- すべての DNS クエリーはクリア テキストで送信されます。グループ ポリシーに **split-dns none** と **default-domain none** コマンドが存在する場合、またはこれらコマンドがグループ ポリシーにはないが、デフォルトのグループポリシーに存在する場合、Cisco Secure Client は他の DNS クエリーすべてをローカル DNS リゾルバにクリアテキストで送信します。

（注） split-dns が指定されていない場合、グループ ポリシーはデフォルトのグループ ポリシー内に存在するスプリット トンネル ドメイン リストを継承します。スプリット トンネリング ドメイン リストの継承を防ぐには、split-dns none コマンドを使用します。

iOS 用の YubiKey 証明書認証

VPN 証明書認証の外部証明書として、YubiKey を使用できます。YubiKey 機能を有効にするには、MDM VPN プロファイルの VendorConfig に以下を追加します。

有効なスロット値 9a、9c、9d、または 9e を指定した YubiKeyCertSlot

YubiKey は他のスマートカード/トークンデバイスと同じではなく、同じサポートもありません。たとえば、Cisco Secure Firewall ASA のデフォルトグループポリシーで設定されている **SmartCard removal disconnect** コマンドは、モバイルデバイスでの YubiKey には影響しません。

iOS での Cisco Secure Client の MDM で設定可能な設定

ベンダーデータを介して VPN xml プロファイルをインポートする

ベンダーデータを介して VPN xml プロファイルを VPN プロファイルにインポートすることができます。次のキー/値ペアで MDM を使用して、デフォルト値を変更し、カスタムデータに追加します。その後、システム設定に移動してプロファイルをインストールし、MDM サーバーからユーザーデバイスにプッシュできます。

最初のキーと値のペアを使用すると、VPN xml プロファイルが渡されます。2 番目のキー/値のペアは、既存のプロファイルが存在する場合、それを置き換えるかどうかを示します。

キー	値
VpnConnectionProfile	[xml プロファイルの文字列]
VpnReplaceExistingProfile	true/false

Cisco Secure Client のローカルセキュア設定の定義

管理対象 Apple iOS デバイスで Cisco Secure Client のローカルセキュア設定を定義するには、次のキーと値のペアで MDM を使用してデフォルト値を変更します。これらのキーまたは値のペアが MDM によって設定されると、エンドユーザのデバイスにプッシュされます。これらの値は MDM 設定で設定され、Cisco Secure Client のエンドユーザーが Cisco Secure Client UI でこれらの設定を変更できないようにします。

キー	値	タイプ
UriExternalControl	Disabled/Prompt/Enabled	文字列
BlockUntrustedServers	true/false	ブール値
EnableFipsMode	true/false	ブール値
CheckCert Revocation	true/false	ブール値
StrictCertTrust	true/false	ブール値

エンドユーザーによる VPN 接続の追加のブロック

Cisco Secure Client エンドユーザーによる管理対象 Apple iOS デバイスへの VPN 接続の追加をブロックするには、BlockUserCreateVPNConnection キーを true の値に設定して MDM を使用します。これらの値は MDM 設定で設定され、Cisco Secure Client エンドユーザーが VPN 接続を追加したり、プロファイルをインポートしたりできないようにします。また、VPN 接続の作成またはプロファイルのインポートのための URI の処理が無効になります。このキーまたは値のペアが MDM で設定されていない場合、エンドユーザーは VPN 接続を追加できます（デフォルト）。

Chrome OS デバイスでの Cisco Secure Client

このリリースでサポートされている機能およびデバイスについては、『Release Notes for Cisco Secure Client, for Google Chrome OS』[英語] を参照してください。

Chrome OS での Cisco Secure Client の注意事項と制約事項

- 今後の Chrome OS リリースは計画していません。現在のすべての ChromeBooks は Android アプリケーションに対応しているため、代わりに Cisco Secure Client Android アプリを使用することをお勧めします。

- Chromebook デバイスを管理すると（Enterprise Chrome Management サービスに登録）、Cisco Secure Client はクライアント証明書にアクセスできず、クライアント証明書認証は機能しません。
- ローエンドの Chromebook では VPN のパフォーマンスが制限されます（Chromium の問題 #514341）。
- 自動再接続（ネットワーク インターフェイスがダウンして回復したときに VPN セッションに再接続する）は、Cisco Secure Client リリース 4.0.10113 以降を Chrome OS 51 以降で使用する場合にサポートされます。Chrome 51 より前は、Wi-Fi を失ったり、デバイスがスリープ状態になったりすると、Cisco Secure Client は自動的に再接続できませんでした。
- Chrome OS 45 以降を使用していない限り、セキュアゲートウェイから受信されたすべてのサーバー証明書が、完全に信頼できる有効なものであっても、信頼できない証明書として表示されます。
- Chrome OS で Cisco Secure Client をインストールまたはアップグレードした後 、初期化によって Cisco Secure Client の設定が完了するまで待機してください。Cisco Secure Client アプリケーションに [初期化しています。しばらくお待ちください....（Initializing, please wait...）] と表示されます。このプロセスに数分かかることがあります。

ユニバーサル Windows プラットフォームでの Cisco Secure Client

このリリースでサポートされている機能およびデバイスについては、『Release Notes for Cisco Secure Client, for Universal Windows Platform』[英語] を参照してください。

ユニバーサル Windows プラットフォームでの Cisco Secure Client の注意事項と制約事項

- DTLS と IPsec/IKEv2 をサポートしていないため、パフォーマンスが限定されます。
- VPN ローミング（WiFi と 3G/4G/5G ネットワーク間の遷移）はサポートされていません。
- ユーザーが開始した接続の切断では、ヘッドエンドからの切断がクリーンに行われません。短いアイドルタイムアウトで Cisco Secure Firewall ASA VPN グループに接続し、Cisco Secure Firewall ASA で孤立したセッションをクリアすることを推奨します。
- 有効なモバイルライセンスがない Cisco Secure Firewall ASA にモバイルデバイスのユーザーが接続すると、クレデンシャルを入力した後に認証が再起動し、最終的に（5 回試行した後）、[VPN の接続はエラーコード 602 で失敗しました（The VPN connection has failed with error code 602）] という一般的なエラーメッセージが送信されるログインループに陥ります。管理者に問い合わせてセキュア ゲートウェイに有効なモバイル ライセンスがインストールされていることを確認してください。

Cisco Secure Firewall ASA ゲートウェイでのモバイルデバイスの VPN 接続の設定

ステップ 1 デスクトップ/モバイルエンドポイントに共通の設定手順については、該当するリリースの『Cisco ASA Series VPN CLI or ASDM Configuration Guides』[英語] を参照してください。モバイル デバイスの場合は以下を考慮してください。

属性	ASDM ロケーション	例外
ホーム ページ URL	[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network（Client）Access）] > [グループ ポリシー（Group Policies）] > [追加/編集（Add / Edit）] > [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] > [カスタマイズ（Customization）]	Cisco Secure Client Mobile は、ホームページの URL 設定を無視します。認証の成功後に、モバイル クライアントをリダイレクトすることはできません。
Cisco Secure Client 接続プロファイル名およびエイリアス	[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] > [追加/編集（Add / Edit）]	Cisco Secure Client モバイルクライアント接続に使用するトンネルグループ（接続プロファイル）の [名前（Name）] または [エイリアス（Aliases）] フィールドに特殊文字を使用しないでください。特殊文字を使用すると、[ゲートウェイからの応答を処理できません（Unable to process response from Gateway）] とログに記録された後、[接続に失敗しました（Connect attempt has failed）] というエラーメッセージが Cisco Secure Client クライアントに表示される場合があります。
デッド ピア検出	[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network（Client）Access）] > [グループ ポリシー（Group Policies）] > [追加/編集（Add / Edit）] > [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）]	サーバー側のデッドピア検出機能はデバイスがスリープ状態になることを防ぐため、オフに切り替えます。ただし、ネットワークの接続性が失われたことによってトンネルが終了したとき、そのことをクライアントが判断できるように、クライアント側のデッドピア検出はオンにしておく必要があります。

属性	ASDM ロケーション	例外
SSL キープアライブ メッセージ	[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network（Client）Access）] > [グループ ポリシー（Group Policies）] > [追加/編集（Add / Edit）] > [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）]	クライアント側のデッド ピア検出がすでに有効になっている場合、モバイルデバイスのバッテリ寿命を延ばすため、これらのキープアライブ メッセージを無効にすることを推奨します。
IPsec over NAT-T キープアライブ メッセージ	[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク(クライアント)アクセス（Network (Client) Access）] > [詳細設定（Advanced）] > [IPsec] > [IKEポリシー（IKE Policies）]	Cisco Secure Client IPsec が機能するようにするには、[IPsec over NAT-Tの有効化（Enable IPsec over NAT-T）] を選択する必要があります。有効にすると、デフォルトでは NAT キープアライブ メッセージが 20 秒ごとに送信されるため、モバイル デバイスのバッテリーが過剰に消費されます。 これらのメッセージを無効にすることはできないため、モバイルデバイスのバッテリ消費への影響を最小限に抑えるには、NAT-T キープアライブを最大値（3600）に設定することを推奨します。 Cisco Secure Firewall ASA CLI でこれを指定するには、`crypto isakmp nat-traversal 3600` コマンドを使用します。

ステップ 2 必要に応じてモバイルの接続を受け入れるか、拒否するか、または制限するようにモバイルポスチャ（AnyConnect Identifier Extensions（ACIDex）とも呼ばれる）を設定します。

適切なリリースの『Cisco ASA Series VPN CLI or ASDM Configuration Guides』[英語] の「*Configuring Endpoint Attributes Used in DAPs*」の手順を参照してください。

例：

接続の確立時に Apple iOS で Cisco Secure Client によりヘッドエンドに送信される属性を次に示します。

```
endpoint.anyconnect.clientversion="4.0.03004";
endpoint.anyconnect.platform="apple-ios";
endpoint.anyconnect.devicetype="iPhone7,2";
endpoint.anyconnect.platformversion="9.0";
endpoint.anyconnect.deviceuniqueid="11025f84e99351e807f3583343bfec96351cb416";
```

ステップ 3 （任意） アプリケーション単位 VPN トンネリングモードを設定します。

「アプリごとの VPN を設定する （31 ページ）」を参照してください。

アプリケーション単位 VPN トンネリングモードが設定されていない場合、Cisco Secure Client アプリケーションはシステムトンネリングモードで動作します。

アプリごとの VPN を設定する

始める前に

Cisco Secure Client アプリごとの VPN トンネリングには次のものが必要です。

- ASA 9.3.1 以降（アプリケーション単位 VPN トンネリングを設定する場合）。
- Cisco Secure Client Advantage または Premier ライセンス

Cisco Secure Client アプリケーション単位の VPN では、次のモバイルプラットフォームがサポートされています。

- Android 5.0（Lollipop）以降を実行している Android デバイス。
- モバイルデバイス管理（MDM）ソリューションでアプリケーション単位 VPN のを使用するように設定されている、Apple iOS 8.3 以降を実行している Apple iOS デバイス。

ステップ 1 Cisco Secure Client 企業アプリケーション セレクタ ツールのインストール （31 ページ）。

ステップ 2 トンネル内で許可する必要のあるアプリケーションの決定 （32 ページ）。

ステップ 3 トンネル内でバイパスする必要のあるアプリケーションの決定 （33 ページ）。

ステップ 4 モバイルアプリのアプリケーション ID の決定 （34 ページ）。

ステップ 5 アプリごとの VPN を設定する （31 ページ）。

ステップ 6 アプリケーション セレクタ ツールを使用して、プラットフォームに対する Cisco Secure Client のアプリケーション単位 VPN ポリシーを指定します。

- Android デバイスでのアプリケーションごとの VPN ポリシーの定義 （35 ページ）
- Apple iOS デバイスのアプリケーション単位 VPN ポリシーの定義 （36 ページ）

ステップ 7 Secure Firewall ASA での アプリケーション単位カスタム属性の作成 （36 ページ）

ステップ 8 Cisco Secure Firewall ASA のポリシーへのカスタム属性の割り当て （37 ページ）。

Cisco Secure Client 企業アプリケーション セレクタ ツールのインストール

アプリケーション セレクタ ツールは、Android デバイスと Apple iOS デバイスの両方のポリシー生成をサポートするスタンドアロン アプリケーションです。

始める前に

Cisco Secure Client 企業アプリケーションセレクタには Java 7 以降が必要です。

ステップ 1 Cisco.com の Cisco Secure Client Software Centerから Cisco Secure Client 企業アプリケーション セレクタ ツールをダウンロードします。

ステップ 2 ポリシーで Android アプリケーションを使用している場合は、Android SDK および Android SDK Build-tools をシステムにインストールしておく必要があります。そうしない場合は、次のようにインストールします。

a) アプリケーション セレクタ ツールが実行されているプラットフォーム用の Android SDK Tools の最新バージョンをインストールします。

デフォルトのパスと設定（[全ユーザー用のインストール（Install for All Users）] が含まれるため、パッケージエンティティへのアクセスは前述のとおりになる）を使用して、プラットフォーム用の推奨された **SDK Tools Only** パッケージをインストールします。

b) Android SDK Manager を使用して、**Android SDK Build-tools** の最新バージョンをインストールします。

次のタスク

（注） アプリケーション セレクタ ツールで要求されたら、インストール場所（*Android SDK* のインストール ディレクトリ\build-tools*build-tools* バージョン番号\）を指定して、Android Asset Packaging Tool（**aapt**）へのアクセスを設定します。

トンネル内で許可する必要のあるアプリケーションの決定

Android または iOS を実行している電話などのモバイルデバイスをサポートする場合は、Mobile Device Manager（MDM）アプリケーションを使用して VPN アクセスを微調整し、サポートされているアプリケーションのみに VPN トンネルの使用を許可できます。リモートアクセス VPN を承認済みアプリケーションに制限することにより、VPN ヘッドエンドの負荷を削減し、これらのモバイルデバイスにインストールされている悪意のあるアプリケーションから企業のネットワークを保護することもできます。

アプリケーションごとのリモートアクセス VPN を使用するには、サードパーティの MDM アプリケーションをインストールして設定する必要があります。これは承認済みアプリケーションのリストを定義する MDM であり、VPN トンネル経由で使用できます。選択したサードパーティ MDM を設定および使用する方法の解説は、このドキュメントの対象範囲外です。

Cisco Secure Client を使用してモバイルデバイスから VPN 接続を確立すると、個人アプリケーションからのトラフィックを含むすべてのトラフィックが VPN 経由でルーティングされます。代わりに企業のアプリケーションのみを VPN 経由でルーティングし、企業以外のトラフィックを VPN から除外する場合は、アプリケーションごとの VPN を使用して、VPN 経由でトンネリングするアプリケーションを選択できます。

アプリケーションごとの VPN を設定すると、次の主要なメリットがもたらされます。

- パフォーマンス：VPN内のトラフィックを企業のネットワークに送信する必要があるトラフィックに制限します。したがって、リモートアクセス VPN のヘッドエンドでリソースを解放できます。
- 保護：承認済みのアプリケーションからのトラフィックのみが許可されるため、ユーザが意図せずモバイルデバイスにインストールした可能性がある未承認の悪意のあるアプリケーションから企業のトンネルを保護します。これらのアプリケーションはトンネルに含まれないため、これらのアプリケーションからのトラフィックはヘッドエンドに送信されません。

モバイルエンドポイントで実行されている Mobile Device Manager（MDM）は、アプリケーションごとの VPN ポリシーをアプリケーションに適用します。

トンネル内でバイパスする必要のあるアプリケーションの決定

代替の設定方法として、Android では MDM を使用してトンネルをバイパスさせるアプリケーションを指定することもできます。指定していない他のすべてのアプリケーションはトンネルを通過します。このオプションは、ルートベースではなくアプリケーションベースの場合を除き、他のプラットフォーム上でスプリット除外と同様の機能があります。

サードパーティのMDMアプリケーションをインストールして設定する必要があります。MDM 内で VPN トンネルをバイパスさせるアプリケーションのリストを定義します。このドキュメントではサードパーティ MDM の設定や使用方法については説明しませんが、モバイルエンドポイントで実行されている MDM では、アプリケーションごとの VPN ポリシーに基づいてアプリケーション除外が適用されます。MDM 内で Android 設定フレームワークのキーと値のペアを設定し、サポートするキーを定義します。MDM を用いた Android の管理設定では、トンネルを通過させるアプリケーションに対して **vpn_connection_allowed_apps** を選択するように、トンネルをバイパスさせるアプリケーションに対しては **vpn_connection_disallowed_apps** を選択します。次に、除外または含めるアプリケーションIDのカンマ区切りリストを入力します。

どちらの設定でも、ヘッドエンドでアプリケーションごとの VPN を有効にする必要があります。次に例を示します。

- `string name="vpn_connection_allowed_apps"`

  トンネリングの対象にするアプリケーションを指定します。これにより、アプリケーションごとの VPN が有効になります。他のすべてのアプリケーションはトンネリングされません。

- `string name="vpn_connection_disallowed_apps"`

  バイパスの対象にするアプリケーションを指定します。これにより、アプリケーションごとの VPN が有効になります。これらのアプリケーションはパブリックインターフェイスで使用できるようになり、他のすべてのアプリケーションはトンネリングされます。

モバイルアプリのアプリケーション ID の決定

ユーザーのモバイルデバイスにサービスを提供するために選択した Mobile Device Manager（MDM）にアプリケーションごとのポリシーを設定することを強く推奨します。これにより、ヘッドエンドの設定が大幅に簡素化されます。

代わりにヘッドエンドで許可するアプリケーションのリストまたはブロックするアプリケーションのリストを設定する場合も、エンドポイントのタイプごとに各アプリケーションの ID を決定する必要があります。

iOS でバンドル ID と呼ばれるアプリケーション ID は、逆引き DNS 名です。ワイルドカードとしてアスタリスクを使用できます。たとえば、*. * はすべてのアプリケーションを示し、com.cisco. * はすべてのシスコアプリケーションを示します。

- Android：Web ブラウザで Google Play に移動し、アプリカテゴリを選択します。許可する（または許可しない）アプリケーションをクリック（またはマウスオーバー）して、URL を確認します。アプリケーション ID は、URL 内の **id=**パラメータに示されます。たとえば、次は Facebook Messenger の URL であるため、アプリケーション ID は com.facebook.orca です。

  ```
  https://play.google.com/store/apps/details?id=com.facebook.orca
  ```

独自のアプリケーションなどの Google Play を通じて入手できないアプリケーションの場合は、パッケージ名ビューアアプリケーションをダウンロードして、アプリケーション ID を抽出します。シスコは、使用可能なアプリケーションのいずれも推奨しませんが、そのうちのいずれかはユーザが必要とするものを提供しているはずです。

- iOS：バンドル ID を検索する 1 つの方法：

  1. Chrome などのデスクトップブラウザを使用して、アプリケーション名を検索します。
  2. 検索結果で、Apple App Store からアプリケーションをダウンロードするためのリンクを探します。たとえば、Facebook メッセンジャー は https://apps.apple.com/us/app/messenger/id454638411 などになります。
  3. **id** 文字列の後に数値をコピーします。この例では、**454638411** です。
  4. 新しいブラウザウィンドウを開き、次の URL の末尾に数値を追加します。

     ```
     https://itunes.apple.com/lookup?id=
     ```

     この例では、https://itunes.apple.com/lookup?id=454638411 です。
  5. 通常は 1.txt という名前のテキストファイルをダウンロードするように求められます。ファイルをダウンロードします。
  6. ワードパッドなどのテキストエディタでファイルを開き、bundleId を検索します。例："bundleId":"com.facebook.Messenger" この例では、バンドル ID は「com.facebook.Messenger」です。これをアプリケーション ID として使用します。

アプリケーション ID のリストを取得したら、ポリシーを設定できます。

Android デバイスでのアプリケーションごとの VPN ポリシーの定義

アプリケーションごとの VPN ポリシーは一連のルールで構成され、各ルールは、どのアプリケーションのデータがそのトンネルを経由するかを特定します。モバイルデバイス環境内で許容されるアプリケーションとその使用方法をより厳密に特定するには、ルールオプションを指定します。アプリケーションごとにMDMが設定されている場合でも、アプリケーションごとに機能させるために、Cisco Secure Firewall ASA でアプリケーションごとのポリシー（カスタム属性）の一部を設定する必要があります。アプリケーションセレクタツールは、アプリケーションパッケージファイル `*.apk` からの情報を使用して、ルールオプションを設定します。Android パッケージマニフェスト情報については、http://developer.android.com/guide/topics/manifest/manifest-element.html を参照してください。

始める前に

Cisco Secure Client 企業アプリケーションセレクタには Java 7 以降が必要です。

ステップ 1 アプリケーション セレクタを起動し、[Android] モバイル デバイス プラットフォームを選択します。

ステップ 2 必須の [アプリケーションID（App ID）] フィールドに値を設定します。

- ローカル システムに保存されているアプリケーションからアプリケーション固有のパッケージ情報をインポートするため、[ディスクからインポート（Import from Disk）] を選択します。

  [アプリケーションID（APP ID）] フィールド（逆 DNS 形式の文字列）には値が自動的に取り込まれます。例えば Apple iOS ポリシーに Chrome アプリケーションを選択した場合、[アプリケーションID（APP ID）] フィールドは **`com.google.chrome.ios`** に設定されます。Android の Chrome の場合、これは **`com.android.chrome`** に設定されます。

- あるいは、アプリケーション固有の情報を直接入力することもできます。

- ワイルドカードを使用した逆 DNS 形式を指定します。たとえば、ルールでアプリケーションを 1 つずつリストする代わりに、すべての Cisco アプリケーションをトンネリングするには com.cisco.* と指定します。ワイルドカードは、[アプリケーションID（APP ID）] のエントリの最後の文字である必要があります。

  管理対象環境でアプリケーションごとの VPN を設定する場合は、Cisco Secure Firewall ASA ポリシーによって、MDM ポリシーと同じアプリケーションのトンネリングが許可されていることを確認します。すべてのアプリケーションのトンネリングを許可するために、アプリケーション ID として *.* を指定し、MDM ポリシーがトンネリングされたアプリケーションの唯一のアービターとなるように確保することを推奨します。*.* 以外のポリシーはサポートされていません。

ステップ 3 （任意） リストされたアプリケーションを選択し、必要に応じてその他のパラメータを設定します。

- [最小バージョン（Minimum Version）]：パッケージのマニフェスト属性 *android:versionCode* で指定された、選択したアプリケーションの最小バージョン。
- [一致証明書 ID（Match Certificate ID）]：アプリケーション署名証明書のダイジェスト。

- [共有 UID を許可（Allow Shared UID）]：デフォルト値は true です。false に設定した場合、パッケージマニフェストで *android: sharedUserId* 属性が指定されたアプリケーションはこのルールに一致せず、トンネルにアクセスできません。

ステップ 4 **[ファイル（File）] > [保存（Save）]** をクリックして、このアプリケーションごとの VPN ポリシーを保存します。

ステップ 5 [ポリシー（Policy）] > [ポリシーの表示（View Policy）] を選択し、定義したポリシーの表示を確認します。

この文字列をコピーします。これは、Cisco Secure Firewall ASA の *perapp* カスタム属性の値になる文字列です。

Apple iOS デバイスのアプリケーション単位 VPN ポリシーの定義

Apple iOS デバイスのアプリケーション単位 VPN のポリシーは MDM 機能で完全に制御されます。したがって、AnyConnect はすべてのアプリケーションを許可する必要があり、MDM はアプリケーション単位のポリシーを設定し、トンネリングできる特定のアプリケーションを指定する必要があります。

始める前に

Cisco AnyConnect 企業アプリケーション セレクタには Java 7 以降が必要です。

ステップ 1 アプリケーション セレクタを起動し、[Apple iOS] モバイル デバイス プラットフォームを選択します。

ステップ 2 必須の [アプリケーションID（App ID）] フィールドを ***.*** に設定します。

この設定により、すべてのアプリケーションを AnyConnect 経由でトンネリングでき、MDM のアプリケーション単位のポリシーが、トンネリングされたアプリケーションの唯一のアービターとなります。

ステップ 3 [ファイル（File）] > [保存（Save）] をクリックして、アプリケーション単位 VPN ポリシーを保存します。

ステップ 4 [ポリシー（Policy）] > [ポリシーの表示（View Policy）] を選択し、定義したポリシーの表示を確認します。

この文字列をコピーします。これは、ASA の *perapp* カスタム属性の値になる文字列です。

アプリケーション単位カスタム属性の作成

ステップ 1 ASDM で、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [詳細（Advanced）] > [AnyConnect カスタム属性（AnyConnect Custom Attributes）] に移動してカスタム属性タイプを設定します。

ステップ 2 [追加（Add）] または [編集（Edit）] を選択し、[カスタム属性タイプの作成/編集（Create / Edit Custom Attribute Type）] ペインで次の設定を行います。

a) タイプとして *perapp* を入力します。

タイプは *perapp* にする必要があります。これは、アプリケーション単位 VPN に関して Cisco Secure Client が認識する唯一の属性タイプであるためです。この属性をリモートアクセス VPN グループプロファイルに追加すると、トンネルが明示的に識別されたプラットフォームに自動的に制限されます。他のすべてのアプリケーションからのトラフィックは、トンネルから自動的に除外されます。

b) 任意の説明を入力します。

ステップ 3 [OK] をクリックして、このペインを閉じます。

ステップ 4 [設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [詳細（Advanced）] > [AnyConnect カスタム属性名（AnyConnect Custom Attribute Names）] に移動してカスタム属性を設定します。

ステップ 5 [追加（Add）] または [編集（Edit）] を選択し、[カスタム属性名の作成/編集（Create / Edit Custom Attribute Name）] ペインで次の設定を行います。

a) *perapp* 属性タイプを選択します。

b) 名前を入力します。 この名前は、ポリシーにこの属性を割り当てるために使用されます。

c) ポリシー ツールから BASE64 形式をコピーしてここに貼り付けて、1 つ以上の値を追加します。

各値は 420 文字を超えることはできません。値がこの長さを超える場合は、追加の値コンテンツ用の複数の値を追加します。設定値は Cisco Secure Client に送信される前に連結されます。

Cisco Secure Firewall ASA のポリシーへのカスタム属性の割り当て

perapp カスタム属性は、グループ ポリシーまたはダイナミック アクセス ポリシーに割り当てることができます。

ステップ 1 Secure Firewall ASA でポリシーを開きます。

- グループポリシーの場合、[設定（Configuration）] > [リモートアクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network（Client）Access）] > [グループポリシー（Group Policies）] > [追加/編集（Add / Edit）] > [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] > [カスタム属性（Custom Attributes）] に移動します。
- ダイナミック アクセス ポリシーの場合、[設定（Configuration）] > [リモートアクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [ダイナミックアクセスポリシー（Dynamic Access Policies）] > [追加/編集（Add / Edit）] に移動します。[アクセス/認証ポリシーの属性（Access/Authorization Policy Attributes）] セクションで、[AnyConnect カスタム属性（AnyConnect Custom Attributes）] タブを選択します。

ステップ 2 既存の属性の [追加（Add）] または [編集（Edit）] をクリックして、[カスタム属性の作成/編集（Create / Edit Custom Attribute）] ペインを開きます。

ステップ 3 ドロップダウン リストから定義済みの *perapp* 属性タイプを選択します。

ステップ 4 [値の選択（Select Value）] を選択し、ドロップダウン リストから定義済みの値を選択します。

ステップ 5 [OK] をクリックして、開いた設定ペインを閉じます。

Cisco Secure Client VPN プロファイルでのモバイルデバイス接続の設定

Cisco Secure Client VPN プロファイルは XML ファイルであり、クライアントの動作を指定し、VPN 接続エントリを識別します。各接続エントリは、このエンドポイント デバイスにアクセス可能なセキュア ゲートウェイとその他の接続属性、ポリシー、および制約を指定します。モバイルデバイスのホスト接続エントリを含むVPNクライアントプロファイルを作成するには、Cisco Secure Client プロファイルエディタを使用します。

Cisco Secure Firewall ASA からモバイルデバイスに配信される VPN プロファイルで定義された接続エントリを、ユーザーが変更したり削除したりすることはできません。ユーザは、手動で作成する接続エントリだけを変更および削除できます。

Cisco Secure Client は、モバイルデバイス上で一度に 1 つの現在の VPN プロファイルのみ維持します。自動または手動の VPN 接続を開始すると、現在のプロファイルが新しい VPN プロファイルによって完全に置き換えられます。ユーザが手動で現在のプロファイルを削除した場合、そのプロファイルは削除され、そのプロファイルに定義されているすべての接続エントリが削除されます。

ステップ 1 基本的な VPN アクセスを設定します。

次の例外を考慮した、デスクトップ/モバイル エンドポイントに共通の手順については、「AnyConnect VPN の設定」を参照してください。

プロファイル属性	例外
自動再接続	Apple iOS 以外のすべてのプラットフォームでは、自動再接続の指定に関係なく、Cisco Secure Client Mobile は常に ReconnectAfterResume を試行します。 Apple iOS の場合のみ、[中断時に接続解除（Disconnect On Suspend）] がサポートされています。[中断時に接続解除（Disconnect On Suspend）] を選択すると、Cisco Secure Client は切断してから、VPN セッションに割り当てられたリソースを解放します。ユーザの手動接続またはオンデマンド接続（設定されている場合）に応答する形でのみ再接続されます。
ローカル LAN へのアクセス	Cisco Secure Client Mobile はローカル LAN アクセス設定を無視し、クライアントプロファイルの設定に関係なく常にローカル LAN アクセスを許可します。

ステップ 2 モバイル固有の属性を設定します。

a) VPN プロファイルで、ナビゲーションウィンドウの [サーバーリスト（Server List）] を選択します。
b) リストに新しいサーバ エントリを追加するには、[追加（Add）] を選択するか、リストからサーバ エントリを選択し、サーバリストの [エントリ（Entry）] ダイアログボックスを開くには、[編集（Edit）] をクリックします。
c) モバイル固有のパラメータを設定します。
d) [OK] をクリックします。

ステップ 3 次のいずれかの方法で VPN プロファイルを配布します。

- VPN 接続のモバイルデバイス設定にクライアントプロファイルをアップロードするように Cisco Secure Firewall ASA を設定します。

  VPN プロファイルを Cisco Secure Firewall ASA にインポートして、グループポリシーに関連付ける方法については、「Cisco Secure Client プロファイルエディタ」の章を参照してください。

- クライアントプロファイルをインポートするために、ユーザーに Cisco Secure Client URI リンクを提供します。（Android および Apple iOS のみ）

  ユーザにこのタイプの展開手順を提供するには、「VPN プロファイルのインポート （48 ページ）」を参照してください。

- モバイルデバイスで [プロファイル管理（Profile Management）] を使用して、Cisco Secure Client プロファイルをユーザーがインポートするようにします。（Android および Apple iOS のみ）

URI ハンドラを使用した Cisco Secure Client アクションの自動化

Cisco Secure Client の URI ハンドラは、他のアプリケーションが Universal Resource Identifiers（URI）形式で Cisco Secure Client にアクション要求を渡すようにします。Cisco Secure Client ユーザー設定プロセスを簡素化するため、URI を Web ページまたは電子メールメッセージにリンクとして埋め込み、これらにアクセスする方法をユーザーに提供します。

始める前に

- Cisco Secure Client の URI ハンドラは、他のアプリケーションが Universal Resource Identifiers（URI）形式で Cisco Secure Client にアクション要求を渡すようにします。

  管理された環境の場合：

  外部制御を有効にすると、ユーザとの対話なしですべての URI コマンドを割り当てることができます。[プロンプト（Prompt）] に設定すると、ユーザには URI のアクティビティが通知され、要求時に許可または禁止します。これらを使用する場合、URI の処理に関連付けられたプロンプトに応答する方法をユーザに知らせる必要があります。MDM で設定値を構成するキーと値は次のとおりです。

  キー - *UriExternalControl*

値 - [有効（Enabled）]、[プロンプト（Prompt）]、または [無効（Disabled）]

（注） 構成設定を MDM で実行してユーザ デバイスにプッシュすると、ユーザによるこの設定の変更は許可されなくなります。

管理されていない環境の場合：

Cisco Secure Client アプリケーションで処理する URI はデフォルトで無効です。モバイル デバイスのユーザは、[外部制御（External Control）] アプリケーション設定を [有効（Enable）] または [プロンプト（Prompt）] に設定することで、この機能を許可します。外部制御を有効にすると、ユーザとの対話なしですべての URI コマンドを割り当てることができます。[プロンプト（Prompt）] に設定すると、ユーザには URI のアクティビティが通知され、要求時に許可または禁止します。

- URI ハンドラ パラメータ値を入力する場合、URL エンコーディングを使用する必要があります。このリンクで示すようなツールを使用して、アクション要求を符号化します。次の例も参照してください。
- URI では `%20` はスペース、`%3A` はコロン（:）、`%2F` はスラッシュ（/）、`%40` はアンパサンド（@）を表します。
- URI のスラッシュは任意です。

次のいずれかのアクションをユーザに指定します。

VPN 接続エントリの生成

この Cisco Secure Client URI ハンドラを使用して、ユーザーの Cisco Secure Client 接続エントリの生成を簡略化します。

anyconnect:[//]**create**[/]**?name**=説明**&host**=サーバ アドレス[**&Parameter1**=値**&Parameter2**=値 ...]

ガイドライン

- *host* パラメータは必須です。その他すべてのパラメータはオプションです。アクションがデバイスで実行されると、Cisco Secure Client は、その *name* と *host* に関連付けられた接続エントリに入力するすべてのパラメータ値を保存します。
- デバイスに追加する各接続エントリの個別のリンクを使用します。単一のリンクで複数の作成接続エントリ アクションを指定することはサポートされていません。

パラメータ

- **name**：Cisco Secure Client のホーム画面の接続リストおよび Cisco Secure Client 接続エントリの [説明（Description）] フィールドに表示される接続エントリの一意の名前。Cisco Secure Client は名前が一意の場合のみ応答します。接続リストに収まるように、半角 24 文字以内

にすることを推奨します。テキストをフィールドに入力する場合、デバイスに表示されたキーボード上の任意の文字、数字、または記号を使用します。文字の大文字と小文字が区別されます。

- **host**：接続する Secure Firewall ASA のドメイン名、IP アドレス、またはグループ URL を入力します。Cisco Secure Client が、このパラメータの値を Cisco Secure Client 接続エントリの [サーバーアドレス（Server Address）] フィールドに挿入します。

```
anyconnect://create/?name=SimpleExample&host=vpn.example.com
anyconnect:create?name=SimpleExample&host=vpn.example.com
```

- **protocol**（任意、指定されていない場合は、デフォルトの SSL になる）：この接続に使用される VPN プロトコル。有効な値は次のとおりです。
  - SSL
  - IPsec

```
anyconnect:create?name=ExampleIPsec&host=vpn.company.com&protocol=IPsec
```

- **authentication**（任意、プロトコルが IPsec のみを指定している場合に適用、デフォルトは EAP-AnyConnect）：IPsec VPN 接続で使用される認証方式。有効な値は次のとおりです。
  - EAP-AnyConnect
  - EAP-GTC
  - EAP-MD5
  - EAP-MSCHAPv2
  - IKE-RSA

- **ike-identity**（authentication が EAP-GTC、EAP-MD5、EAP-MSCAPv2 に設定されている場合に必要）：AUTHENTICATION が EAP-GTC、EAP-MD5 または EAP-MSCHAPv2 に設定されているときの IKE ID。このパラメータは、他の認証設定に使用されたときに無効になります。

```
anyconnect:create?name=Description&host=vpn.company.com&protocol=IPsec
&authentication=eap-md5&ike-identity=012A4F8B29A9BCD
```

- **netroam**（任意、Apple iOS にのみ適用）：デバイスの起動後または接続タイプ（EDGE、3G、Wi-Fi など）の変更後、再接続にかかる時間を制限するかどうかを決定します。このパラメータは、データローミングまたは複数のモバイル サービス プロバイダーの使用には影響しません。有効な値は次のとおりです。
  - true：（デフォルト）このオプションは VPN アクセスを最適化します。接続エントリの Network Roaming フィールドに値 ON を挿入します。Cisco Secure ClientCisco Secure ClientCisco Secure Client が接続を失った場合、成功するまで新しい接続の確立が試行されます。この設定により、アプリケーションは VPN への持続的な接続に依存できます。Cisco Secure Client は再接続にかかる時間を制限しません。
  - false：このオプションでは、バッテリ寿命が最適化されます。Cisco Secure Client はこの値を Cisco Secure Client 接続エントリの [ネットワークローミング（Network Roaming）] フィールドの OFF 値と関連付けます。Cisco Secure Client が接続を失った

場合、新しい接続の確立が 20 秒間試行され、その後試行が停止されます。ユーザまたはアプリケーションは、必要な場合は新しいVPN接続を開始する必要があります。

```
anyconnect:create?name=Example%201&host=vpn.example.com&netroam=true
```

- **keychainalias**（任意）：システムの証明書ストアから Cisco Secure Client の証明書ストアに証明書をインポートします。このオプションは、Android のモバイル プラットフォーム専用です。

  名前の付いた証明書がまだシステムストアに存在しない場合、ユーザーは証明書を選択してインストールするように求められ、その後、Cisco Secure Client ストアへのコピーを許可または拒否するかを求めるプロンプトが表示されます。モバイルデバイスで外部制御を有効にする必要があります。

  次の例では、IP アドレスが *vpn.example.com* に設定され、認証用に *client* という名前の証明書が割り当てられている *SimpleExample* という名前の新しい接続エントリを作成します。

  ```
  anyconnect://create/?name=SimpleExample&host=vpn.example.com&keychainalias=client
  ```

- **usecert**（任意）：ホストへの VPN 接続を確立するときに、デバイスにインストールされているデジタル証明書を使用するかどうかを決定します。有効な値は次のとおりです。

  - true（デフォルト設定）：ホストとのVPN接続を確立するときに自動証明書選択を無効化します。[証明書（Certificate）] フィールドを自動にする certcommonname 値を指定することなしに usecert を true に返し、接続時に Cisco Secure Client 証明書ストアから証明書を選択します。

  - false：自動証明書の選択を無効化します。

  ```
  anyconnect:create?name=Example%201&host=vpn.example.com&usecert=true
  ```

- **certcommonname**（任意、ただし isecert パラメータは必要）：デバイスにあらかじめインストールされた有効な証明書の共通名を照合します。Cisco Secure Client はその値を Cisco Secure Client 接続エントリの [証明書（Certificate）] フィールドに挿入します。

  デバイスにインストールされているこの証明書を表示するには、**[診断（Diagnostics）]** > **[証明書（Certificates）]** をタップします。host によって要求された証明書を表示するには、スクロールが必要な場合があります。証明書から読み取った共通名パラメータ、およびその他の値を表示するには、詳細表示ボタンをタップします。

- **useondemand**（任意、Apple iOS だけに適用、usercert、certcommonname パラメータ、および下記のドメイン指定が必要）：Safari などのアプリケーションが、VPN 接続を開始できるかどうか決定します。有効な値は次のとおりです。

  - false（デフォルト）：アプリケーションはVPN接続を開始できません。このオプションは、DNS 要求を行うアプリケーションが VPN 接続をトリガーしないようにする唯一の手段です。Cisco Secure Client は、このオプションを Cisco Secure Client 接続エントリの[オンデマンド接続（Connect On Demand）] フィールドの OFF 値に関連付けます。

  - true：アプリケーションはApple iOSを使用してVPN接続を開始できます。useondemand パラメータを true に設定すると、Cisco Secure Client は値 ON を Cisco Secure Client 接

続エントリの [オンデマンド接続（Connect on Demand）] フィールドに挿入します。（useondemand=true の場合、domainlistalways パラメータまたは domainlistifneeded パラメータは必須）

```
anyconnect:create?name=Example%20with%20certificate&host=vpn.example.com
&netroam=true&usecert=true&certcommonname=example-ID&useondemand=true
&domainlistalways=email.example.com,pay.examplecloud.com
&domainlistnever=www.example.com&domainlistifneeded=intranet.example.com
```

- **domainlistnever**（オプション、useondemand=true が必要）：オンデマンド接続機能の使用を不適格とするために、一致を評価するドメインをリストにまとめます。このリストは、ドメイン要求の一致を評価する場合に Cisco Secure Client が最初に使用するリストです。ドメインリクエストが一致する場合、Cisco Secure Client は、ドメインリクエストを無視します。Cisco Secure Client は、このリストを Cisco Secure Client 接続エントリの [接続しない（Never Connect）] フィールドに挿入します。このリストを使用して、特定のリソースを除外できます。たとえば、公開されている Web サーバ経由では自動 VPN 接続を許可しない場合などが考えられます。値は `www.example.com` などのように指定します。
- **domainlistalways**（useondemand=true の場合、domainlistalways または domainlistifneeded パラメータが必要）：オンデマンド接続機能について一致を評価するドメインをリストします。このリストは、ドメイン要求の一致を評価する場合に Cisco Secure Client が 2 番目に使用するリストです。アプリケーションがこのパラメータで指定されたいずれかのドメインへのアクセスを要求し、VPN 接続がまだ行われていない場合、Apple iOS は VPN 接続を確立しようとします。Cisco Secure Client はこのリストを Cisco Secure Client 接続エントリの [常に接続（Always Connect）] フィールドに挿入します。値リストの例は `email.example.com,pay.examplecloud.com` です。
- **domainlistifneeded**（useondemand=true の場合、domainlistalways または domainlistifneeded パラメータが必要）：DNS エラーが発生した場合、Cisco Secure Client はこのリストに対してドメイン要求が一致しているかどうか評価します。このリストの文字列がドメインに一致する場合、Apple iOS は VPN 接続の確立を試みます。Cisco Secure Client は、このリストを Cisco Secure Client 接続エントリの [必要に応じて接続（Connect if Needed）] フィールドに挿入します。このリストの最も一般的な用途は、社内ネットワーク内の LAN ではアクセスできない内部リソースへの短時間のアクセス権を取得することです。値は `intranet.example.com` などのように指定します。

カンマで区切ったリストを使用して、複数のドメインを指定します。Connect-on-Demand の規則は IP アドレスではなく、ドメイン名のみサポートしています。ただし Cisco Secure Client は、各リストエントリのドメイン名形式について次のような柔軟性があります。

一致	指示	エントリの例	一致する例	一致しない例
プレフィックスおよびドメイン名が正確に一致。	プレフィックス、ドット、ドメイン名を入力します。	email.example.com	email.example.com	www.example.com email.1example.com email.example1.com email.example.org

一致	指示	エントリの例	一致する例	一致しない例
ドメイン名は正確に一致し、プレフィックスは任意。先頭にドットを付けると、*example.com で終わるホスト（notexample.com など）への接続を防止できます。	ドットに続けて、照合するドメイン名を入力します。	.example.org	anytext.example.org	anytext.example.com anytext.1example.org anytext.example1.org
指定したテキストで終わる任意のドメイン名。	照合するドメイン名の最後の部分を入力します。	example.net anytext	anytext-example.net anytext.example.net	anytext.example1.net anytext.example.com

VPN 接続の確立

VPN に接続してユーザーが容易に VPN 接続を確立できるようにするには、この Cisco Secure Client URI ハンドラを使用します。また、URI に次のタスクを実行するための追加情報を埋め込むことができます。

- ユーザ名とパスワードの事前入力
- 二重認証用のユーザ名とパスワードの事前入力
- ユーザ名とパスワードの事前入力および接続プロファイル エイリアスの指定

このアクションには name または host のいずれかのパラメータが必要ですが、次の構文のいずれかを使用して両方を指定することもできます。

anyconnect:[//]**connect**[/]**?**[**name=**説明|**host=**サーバアドレス][**&Parameter1**=値**&Parameter2**=値..]

または

anyconnect:[//]**connect**[/]**?name=**説明**&host=**サーバアドレス[**&Parameter1**=値**&Parameter2**=値..]

ガイドライン

- ステートメントのすべてのパラメータ値がデバイスの Cisco Secure Client 接続エントリに一致する場合、Cisco Secure Client は接続を確立するために残りのパラメータを使用します。

- ステートメントのすべてのパラメータが接続エントリのパラメータと一致せず、name パラメータが一意の場合、Cisco Secure Client は新しい接続エントリを生成し、VPN 接続を試行します。
- URI を使用して、VPN 接続を確立するためにワンタイム パスワード（OTP）インフラストラクチャとの組み合わせのみ使用する必要がある場合、パスワードを指定します。

パラメータ

- **name**：Cisco Secure Client ホームウィンドウの接続リストに表示される、接続エントリの名前。Cisco Secure Client はこの値を Cisco Secure Client 接続エントリの [説明（Description）] フィールドに対して評価し、前回の手順を使用してデバイスに接続エントリを作成した場合、name とも呼ばれます。この値は大文字と小文字が区別されます。
- **host**：Cisco Secure Client 接続エントリの [サーバーアドレス（Server Address）] フィールドと一致させるには、Cisco Secure Firewall ASA のドメイン名、IP アドレス、またはグループ URL を入力します。前回の手順を使用してデバイスに接続エントリを生成した場合、host とも呼ばれます。

  グループ URL は、[設定（Configuration）] > [リモートアクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] > [詳細（Advanced）] > [グループ エイリアス/グループ URL（Group Alias/Group URL）] > [グループ URL（Group-URL）] を選択して、ASDM に設定されます。
- **onsuccess**：接続が正常である場合にこのアクションを実行します。プラットフォーム固有の動作は次のとおりです。
  - Apple iOS デバイスの場合、この接続が接続状態に遷移するとき、または anyconnect:close コマンドを使用して Cisco Secure Client GUI を閉じるときに表示される URL を指定します。
  - Android デバイスの場合、この接続が遷移するとき、またはすでに接続状態であるときに表示する URL を指定します。複数の onsuccess アクションを指定できます。Cisco Secure Client は、Android デバイスでの接続が成功した後で常に GUI を閉じます。
- **onerror**：接続に失敗した場合にこのアクションを実行します。プラットフォーム固有の動作は次のとおりです。
  - Apple iOS デバイスの場合、この接続が失敗したとき、または anyconnect:close コマンドを使用して Cisco Secure Client GUI を閉じるときに表示される URL を指定します。
  - Android デバイスの場合、この接続が失敗したときに表示される URL を指定します。複数の onerror アクションを指定できます。Cisco Secure Client は、Android デバイスでの接続が失敗した後で常に GUI を閉じます。
- **prefill_username**：connect URI にユーザ名を指定し、接続プロンプトに自動入力します。

- **prefill_password**：connect URI にパスワードを指定し、接続プロンプトに自動入力します。このフィールドは、ワンタイムパスワード用に設定した接続プロファイルでの使用のみとしてください。
- **prefill_secondary_username**：二重認証を必要とするように設定されている環境では、このパラメータは connect URI でセカンダリ ユーザ名を指定し、接続プロンプトに自動入力します。
- **prefill_secondary_password**：二重認証を必要とするように設定されている環境では、このパラメータは connect URI でセカンダリ ユーザ名のパスワードを指定し、接続プロンプトに自動入力します。
- **prefill_group_list**：これは、[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] > [詳細（Advanced）] > [グループエイリアス/グループURL（Group Alias/Group URL）] > [接続エイリアス（Connection Aliases）] を選択して、ASDM で定義されている接続エイリアスです。

例

- URI に接続名およびホスト名またはグループ URL を入力します。

```
anyconnect://connect/?name=Example

anyconnect:connect?host=hr.example.com

anyconnect:connect?name=Example&host=hr.example.com

anyconnect://connect/?name=Example&host=hr.example.com/group-url
&prefill_username=user1&prefill_password=password1
```

- 成功または失敗に対するアクションの指定

  connect アクションの結果に基づいて特定の URL ベースを開始するために、onsuccess または onerror パラメータを使用します。

```
anyconnect://connect?host=vpn.company.com
&onsuccess=http%3A%2F%2Fwww.cisco.com

anyconnect://connect?host=vpn.company.com
&onerror=http%3A%2F%2Fwww.cisco.com%2Ffailure.html
&onsuccess=http%3A%2F%2Fwww.cisco.com
```

  Android では複数の onsuccess アクションを指定できます。

```
anyconnect://connect?host=vpn.company.com
&onerror=http%3A%2F%2Fwww.cisco.com%2Ffailure.html
&onsuccess=http%3A%2F%2Fwww.cisco.com
&onsuccess=tel:9781111111
```

  Apple iOS デバイスでは、onsuccess パラメータまたは onerror パラメータで anyconnect://close コマンドを使用して、Cisco Secure Client GUI を閉じることができます。

```
anyconnect://connect?host=vpn.company.com
&onsuccess=anyconnect%3A%2F%2Fclose
```

- URI での接続情報の指定およびユーザ名とパスワードの自動入力：

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
```

```
anyconnect:connect?name=Example&host=hr.example.com/group-url
&prefill_username=user1&prefill_password=password1
```

- 二重認証のための接続情報の指定およびユーザ名とパスワードの自動入力：

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
&prefill_secondary_username=user2&prefill_secondary_password=password2
```

- 接続情報の指定、ユーザ名とパスワードの自動入力、および接続プロファイルエイリアスの指定：

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
&prefill_group_list=10.%20Single%20Authentication
```

VPN からの接続解除

VPN からユーザーの接続を解除するには、この Cisco Secure Client URI ハンドラを使用します。

anyconnect:[//]**disconnect**[/]**&onsuccess=**URL

パラメータ

onsuccess パラメータは、Android デバイスだけに適用されます。この接続が解除されるとき、またはすでに接続解除状態であるときに表示される URL を指定します。

例

```
anyconnect:disconnect
```

証明書のインポート

この URI ハンドラ コマンドを使用して、PKCS12 符号化証明書バンドルをエンドポイントにインポートします。Cisco Secure Client は、エンドポイントにインストールされた PKCS12 符号化証明書を使用して自ら Cisco Secure Firewall ASA に認証を行います。PKCS12 証明書タイプのみをサポートします。

anyconnect:[//]**import**[/]**?type=pkcs12&uri=***http%3A%2F%2Fexample.com%2Fcertificatename.p12*

パラメータ

- **type**：PKCS12 証明書タイプのみをサポートします。
- **uri**：証明書がある場所の URL エンコード ID。

例

```
anyconnect:import?type=pkcs12&uri=http%3A%2F%2Fexample.com%2FCertName.p12
```

VPN プロファイルのインポート

Cisco Secure Client にクライアントプロファイルを配布するため、この URI ハンドラ方式を使用します。

anyconnect:[//]**import**[/]**?type=profile&uri=***filename.xml*

例

```
anyconnect:import?type=profile&uri=file%3A%2F%2Fsdcard%2Fprofile.xml
```

Cisco Secure Client UI とメッセージのローカライズ

Cisco Secure Client をローカライズするには、この URI ハンドラ方式を使用します。

anyconnect:[//]**import**[/]**?type=localization&lang=***LanguageCode***&host=**へ

パラメータ

インポート アクションには、すべてのパラメータが必要です。

- **type**：インポートのタイプ（この場合はローカリゼーション）。
- **lang**：anyconnect.po ファイルで指定されて言語を表す 2 文字または 4 文字の言語タグ。たとえば、言語タグは単純に「フランス語」なら fr、「カナダ フランス語」なら fr-ca となります。
- **host**：Cisco Secure Client 接続エントリの [サーバーアドレス（Server Address）] フィールドと一致させるには、Cisco Secure Firewall ASA のドメイン名または IP アドレスを入力します。

例

```
anyconnect:import?type=localization&lang=fr&host=asa.example.com
```

モバイルデバイスでの Cisco Secure Client のトラブルシューティング

始める前に

モバイルデバイスでログを有効にします。

ステップ 1 同じ問題がデスクトップ クライアントまたは別のモバイル OS で発生するかどうかを確認します。

ステップ 2 適切なライセンスが Cisco Secure Firewall ASA にインストールされていることを確認します。

ステップ 3 証明書認証が失敗する場合は、次のことを確認してください。

a) 適切な証明書が選択されていることを確認します。
b) デバイスのクライアント証明書に Extended Key Usage として Client Authentication があることを確認します。
c) Cisco Secure Client プロファイルの証明書一致規則によってユーザーの選択した証明書を除外されていないことを確認します。

   ユーザが証明書を選択しても、プロファイルのフィルタリング ルールに一致しなければ認証には使用されません。

d) 認証メカニズムで Cisco Secure Firewall ASA に関連するアカウンティングポリシーが使用されている場合、ユーザーが正常に認証できることを確認します。
e) 証明書のみの認証を使用しようとしている場合に認証画面が表示されたら、グループ URL を使用するよう接続を設定し、トンネル グループのセカンダリ認証が設定されていないことを確認します。

ステップ 4 Apple iOS デバイスで、次のことを確認します。

a) デバイスが起動した後でVPN接続がリストアされていない場合は、[ネットワーク ローミング（Network Roaming）] が無効になっていることを確認します。
b) Connect On Demand を使用している場合は、証明書のみの認証およびグループ URL が設定されていることを確認します。

次のタスク

それでも問題が解決されない場合は、クライアントのロギングを有効にし、Cisco Secure Firewall ASA のデバッグロギングを有効にします。詳細については、適切なリリースの 『Cisco ASA Series VPN CLI or ASDM Configuration Guide』[英語] を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。